

# Open Source Intelligence in the Twenty-First Century

## New Approaches and Opportunities

Edited by

Christopher Hobbs, Matthew Moran and Daniel Salisbury

*Centre for Science and Security Studies, King's College London, UK*

# 7

## Human Security Intelligence: Towards a Comprehensive Understanding of Complex Emergencies

*Fred Bruls and A. Walter Dorn*

### Introduction

Humanitarian crises may arise from natural disasters, such as droughts, floods and earthquakes, or they may be caused or exacerbated by human beings through armed conflict. The latter are often referred to as 'complex emergencies'. These emergencies call for holistic international responses that need to be coordinated across the variety of humanitarian and military actors. The responses require a great deal of information, situational awareness and occasionally secret intelligence. But the information contained in open sources usually provides ample basis for those organisations seeking to respond positively to these crises.

This chapter seeks to provide an overview of a new and much needed intelligence concept, Human Security Intelligence (HSI), the reasons for its utility and some of the issues arising from its use.<sup>1</sup> It will begin by providing an overview of the international operations that seek to deal with complex emergencies, namely peace operations (POs), before analysing some of the current, flawed and incomplete intelligence practices. The new intelligence concept, HSI, will be introduced as a means to develop a broader understanding of the environment, an understanding that is centred on the civilian populace. OSINT, it will be argued, is a key information source for the HSI model. The production of HSI requires a multidisciplinary and multi-agency approach. In particular, military forces need to work with other agencies to develop effective responses based on strong civil-military cooperation. From this new paradigm arise many questions: How should HSI be managed to enable optimum collaboration? How should information be prioritised in this complex and information-rich environment? The chapter will seek to elaborate on these and other questions, and suggest how HSI can make POs more effective, especially as they have evolved to undertake enormous mandates in the twenty-first century, when the challenges remain daunting.

## Complex intelligence and evolving peace operations

Complex emergencies have been defined by the International Federation of Red Cross and Red Crescent Societies (IFRC) as a state of 'total or considerable breakdown of authority resulting from internal or external conflict and which requires an international response that goes beyond the mandate or capacity of any single agency and/or the ongoing UN country program'.<sup>2</sup> The IFRC goes on to characterise a complex emergency as involving<sup>3</sup>:

- extensive violence and loss of life;
- displacements of populations;
- widespread damage to societies and economies.

The Red Cross also highlights key issues of concern in the humanitarian response:

- the need for large-scale, multifaceted assistance;
- the hindrance or prevention of assistance by political and military constraints;
- significant security risks for relief workers in some areas.

Complex emergencies involve humanitarian actors, such as relief agencies on the ground, and often necessitate the creation of peace operations, especially following the conclusion of a peace agreement or tentative understanding between the conflicting parties.<sup>4</sup> These POs are launched by the UN or regional organisations in order to create a safe and secure environment for the local populace and to help to build the physical and social infrastructure required for a sustainable peace. With such a complex mandate, these operations must coordinate their actions with and among a range of actors, especially the conflicting parties and those involved in local governance. POs are an important means of working towards an integral solution to complex emergencies.

In today's POs, military forces are confronted with new concerns in comparison with more traditional peacekeeping operations, which were usually located on state borders to separate standing armies. Current conflicts, by contrast, are characterised by:

- an increasing number of non-state actors<sup>5</sup>;
- ethnic, religious or cultural disputes throughout large regions or countries;
- asymmetry as opposed to symmetry in the combatant forces – for example, insurgents versus a government; insurgents are often not distinguishable from the local populace in which they seek sanctuary; their modus operandi can include terrorism and the use of proxy forces<sup>6</sup>;

- the need for international interveners to secure the 'goodwill' and support of the populace; this is the new 'centre of gravity' for modern POs<sup>7</sup>; this goodwill is based on the perceived legitimacy of the intervention force; actions deemed inappropriate for the local populace, especially 'collateral damage' or civilian casualties, can rapidly erode this perceived legitimacy;
- diversity of intervening actors, not only military peacekeepers in the field, but including a large number of international (UN) agencies and NGOs; since unity of effort between all of these actors is a key for success in humanitarian operations, coordination and negotiation are extremely important daily activities<sup>8</sup>;
- privatisation of the security sector, in overseas operations and in the host country; private security companies (PSCs) have become significant players in the international operations and even for the combatants; estimates put the total value of the private military and security industry at USD 210 billion in 2010<sup>9</sup>; their clients include both states, international organisations and NGOs, that contract out specific tasks, such as the protection of compounds, buildings, convoys and personnel<sup>10</sup>; local authorities also often hire PSCs for their own protection; PSCs also employ large numbers of local personnel, giving them both influence and intelligence at the local level; for example, it is estimated that in Afghanistan some 90 PSCs are active, employing over 20,000 Afghan personnel.<sup>11</sup>

The increased number of actors and complexity of armed conflicts has led to a significant evolution in POs. More traditional peacekeeping operations, such as the UN Peacekeeping Force in Cyprus (UNFICYP) or the Multilateral Force and Observers (MFO) in the Sinai, took place in a predefined area of responsibility (AOR), consisting of a buffer or demarcation zone between the belligerents. These parties had usually retreated behind fortified lines and had agreed to the presence of the peacekeeping forces. The AOR was mostly uninhabited, due to evacuations of the civil populace. The security of the local populace within the AOR was therefore of less importance.

The more complex peacekeeping operations of the twenty-first century have to deal with the multifaceted problems of complex emergencies. Experience has taught the world that, although the belligerent parties may have agreed to a ceasefire and a peacekeeping force, they also often breach and renege on their agreements. Much more is needed to secure the peace: a functioning society that offers strong political, economic and social alternatives to war. Belligerents also need to be effectively deterred from returning to active hostilities.

Because of this, modern peace operations have largely abandoned the restrictive Rules of Engagement (ROE) found in traditional peacekeeping operations. They have become more robust, including larger forces, such as the Intervention Brigade in the United Nations Stabilization Mission

in the Democratic Republic of the Congo (MONUSCO). In these more complex peacekeeping operations, peacekeeping forces are deployed countrywide instead of on state borders or in no-man's land.<sup>12</sup> Reflecting these changes, new terms have been introduced to describe the various evolving tasks of POs, including peacemaking (negotiations for peace); peace-building (developing the physical and social infrastructure for a sustainable peace); peacekeeping (providing security); peace enforcement (to apply force to stop or reverse of aggression); and preventive deployment (to stop aggression before it occurs).

The consent of all belligerent parties, although an important prerequisite for the initial deployment of a UN peace operation, no longer blocks intervention when circumstances demand the protection of civilians (POC) or enforcement of UN Security Council resolutions.<sup>13</sup> Increasingly, POs use armed force to deal with troublesome 'spoilers' of the peace process. Examples of robust peacekeeping and peace-enforcement operations with robust mandates can be found in Mali, Côte d'Ivoire and the Democratic Republic of the Congo. Although the NATO operations in Afghanistan cannot be labelled as POs, such counterinsurgency operations share common characteristics with POs, and hence can be useful for extracting lessons. Conversely, the UN Assistance Mission in Afghanistan (UNAMA) is an example of a small PO that may in the future expand but has not yet deployed an armed force of its own.

Given the complexity of the environment in which POs take place, and the multiplicity of actors involved, many different facets must be taken into account when planning for missions within the AOR. Current and accurate intelligence is required to understand this environment and for the planning, execution and evaluation of POs. The intelligence branches of the POs are responsible for providing an understanding of the background and current situation in the AOR, and for providing the mission leaders with a common operational picture (COP). According to military doctrine, the COP constitutes a 'snapshot in time' of the mission environment and all military forces present (friendly, hostile and neutral) therein. The COP contributes situational awareness to the commanders, which is their understanding of the mission environment in the context of their mission.<sup>14</sup>

Intelligence models used in the past and present are, however, insufficient to provide a comprehensive understanding of complex emergencies. Given that warfare has moved from predominantly rural to urbanised terrain, the intelligence effort must shift from the 'physical terrain' to the 'human terrain'. The populace has become an extremely important factor for operational success of a peace operation.<sup>15</sup> Which parties do armed persons belong to, which groups do they support and why? What are the threats that confront the populace? What indigenous knowledge, traditions and systems can contribute to a sustainable end state that is acceptable to the various parties and groups? The populace in wartorn countries is traumatised, an aspect

mutually shared by all the communities and groups.<sup>16</sup> A new paradigm offers the possibility of increasing the scope and effectiveness of intelligence and hence the perceived legitimacy of the overall operation. Unfortunately, most approaches in these operations, whether they are taken by the military, the UN or NGOs, are self-centred, resulting in a fragmented picture and stove-piped mission approach, thereby eroding the mission's legitimacy in the eyes of the populace.<sup>17</sup> For instance, resorting solely to military force is considered to be one of the worst options to influence behaviour. More intelligent and intelligence-driven means are required.

### The concept of human security intelligence

Because of the multidimensional nature of modern conflicts and of international responses, those taking part in POs need much stronger information and intelligence-gathering capabilities across the full spectrum of human activities. Because peace is holistic, the mission must also be. A comprehensive understanding of the total operational environment is needed across all domains, not solely the military domain. Still, intelligence professionals must prioritise the most relevant information. To do this, various intelligence models are currently being operationalised by Western forces but these are inadequate.

In traditional war-fighting and peacekeeping operations, military actors focused almost exclusively on threats to physical security, which usually meant watching or targeting opposing military forces. But in the present day's enlarged agenda, the threats are not merely posed by armed attacks against one's own forces; they are also psychological, political, economic and cultural threats to local civilians. To the goal of 'freedom from fear' must be added 'freedom from want', allowing the population not only to survive but also to thrive so that peace can be sustained. The interconnection between these two goals necessitates an interconnected framework, as shown in Figure 7.1.

Given the relationship between the freedom-from-fear and freedom-from-want dimensions, the Common Operational Picture (COP) must cover all factors of human security, putting the civilian populace at the centre.<sup>18</sup> A large range of factors influence events in the AOR and its direct surroundings. Because of this a larger area of interest (AOI) needs to be defined to encompass them.<sup>19</sup> One of the main tasks of intelligence staff – military, police and civilian, whether combined into one organisation or not – is to provide the mission leader with a detailed yet prioritised COP at many levels.

The intelligence models which are most frequently applied in current Western military operations are insufficient to analyse the human security situation in an AOI. The HSI model, an alternative to existing models, is presented, based on the broad definition of human security, as provided by

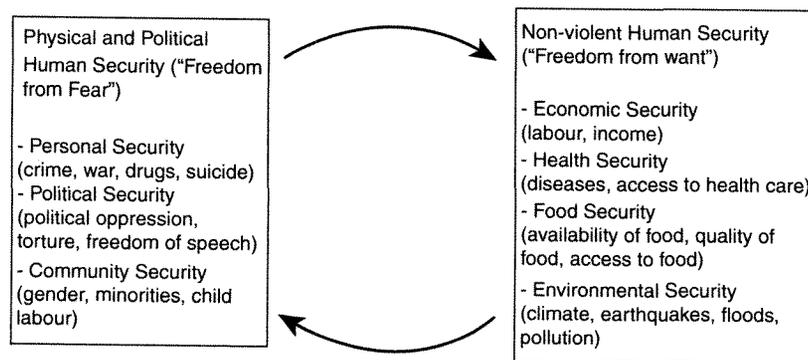


Figure 7.1 Causal pathways of human security<sup>20</sup>

the 1994 *Human Development Report*.<sup>21</sup> If correctly tested and applied, this model could serve as a key early warning mechanism to help to alert humanitarian actors and allow them to prevent the escalation of complex emergencies as well as to resolve them. The existing models needs much improvement.<sup>22</sup>

### Intelligence models in today's operations

Most intelligence staff of Western militaries use various combinations of the models set out in US Army doctrine in order to develop an understanding of the operational environment. These US models are mostly based on so-called 'instruments of national power' that can be used to achieve 'theatre, national and/or multinational objectives'.<sup>23</sup> These intelligence models, which list the principle factors to be analysed, are known by acronyms like DIME, DIMEFIL, ASCOPE and PMESII.<sup>24</sup> Today, DIME and DIMEFIL, though still well known in military circles, are hardly used in POs.<sup>25</sup> The others are still in frequent use and are worth summarising.

The ASCOPE model is currently used in some peace and stabilisation operations. For example, this analytical tool was used by the UK and Australian intelligence communities in Afghanistan. The ASCOPE model analyses the civil aspects<sup>26</sup> of the AOI in the following dimensions<sup>27</sup>:

- areas: analysis of the influence of key civilian areas on military operations and vice versa;
- structures: analysis of physical infrastructure, such as buildings, bridges, roads, railways and communication towers; also the presence of possible toxic materials is taken into account;
- capabilities: analysis of the capabilities required and present in the AOI to save, sustain and enhance life, such as public administration, food, emergency services and health care;

- organisations: analysis of presence, activities and organisational composition of non-military groups and institutions in the AOI with respect to their influence on the populace, the military mission and vice versa;
- people: analysis of non-military people in the AOI in terms of opinions, actions and political influence;
- events: analysis of events in the AOI that affect the populace, military operations, non-military organisations, religious and national holidays, crop harvest and elections; also unplanned events such as civil unrest, environmental or natural disasters, and industrial accidents are taken into account.

The US Army Field Manual 3-0, which sets out the fundamentals of war-fighting, focuses strongly on the PMESII model for the variables affecting operations.<sup>28</sup> Because of this, PMESII has become a standard in peace and stabilisation operations conducted by NATO countries, although the model was not originally intended for adoption in these operations.<sup>29</sup> For example, in Afghanistan, PMESII was used as the intelligence standard for the US and Dutch forces.<sup>30</sup> The PMESII model can be used to analyse the operational side of the AOI.<sup>31</sup> The dimensions explored by this model are<sup>32</sup>:

- political: analysis of political organisations, groups and individuals and their linkages within the AOI;
- military: analysis of military organisations and their capabilities in the AOI;
- economic: analysis of the economic position and health of groups in the AOI;
- social: analysis of social networks within and between groups and social links of individuals;
- information: analysis of the information position of a group in terms of the information known by the group, use of information within the group, propaganda, news media and so on;
- infrastructure: analysis of the infrastructure within the AOI in terms of roads, railways, airports, power supply, sanitation, capabilities like governance organisations and so on.

Often the basic PMESII model is extended with a number of extra dimensions, such as physical environment, time, crime, narcotics or others relevant to the specific mission. Philosophically, this model views the operational environment as a system of interacting subsystems. For example, ethnic or religious groups are viewed as separate interacting systems. These groups are further composed of tribes that are considered to be systems in their own right. Terrorist groups operating in the AOI are also considered to be influencing systems. This philosophy, referred to as the 'system of systems approach', provides the intelligence community with a powerful instrument with which to analyse the AOI.<sup>33</sup>

## Shortcomings of the present intelligence models

The effectiveness of the aforementioned intelligence models in humanitarian and peace operations is, however, limited by a number of factors. First, the models were developed to influence opposing parties or regimes, rather than to address the root causes of crises. The models are enemy-centric or military-centric rather than population-centric. While these factors may be important in the planning process, they are not necessarily linked directly to the desired end state (the security, peace and wellbeing of the population) and thus give only partial guidance to achieve that end state.

A related problem is with the application of the models. They are linear models, meaning that analysis is conducted along a fixed line. For example, in the case of PMESII the line starts with the 'political' dimension and ends with the 'infrastructure' dimension. Admittedly, intelligence analysis often consists of sorting gathered information into the various dimensions. Reality, however, is not linear and not so easily categorised. Linear models limit the flexibility of the analysis and can create an impression of 'static variables within static frameworks' while in reality the operation needs to be dynamic to succeed.<sup>34</sup> This can cause the model and its variables to be misapplied in different circumstances where the context is very different, notably peacekeeping instead of war-fighting.

US Army Field Manual 3-0<sup>35</sup> extends the PMESII model by adding physical environment and time (PMESII-PT) to include more context in the model for intelligence analysis. However, even extending PMESII in this way does not lead to a model providing a more dynamic understanding of the situation, since the model still requires that gathered information is sorted into different dimensions. Area and time are considered as discrete dimensions, and the connection of these with the others (within PMESII) is not analysed.

The second problem in the application of the standard PMESII-type models is that it does not require analysts to consider the broader context. Dimensions like culture, demographics and others go unanalysed, though some of these may be encompassed in the social dimension.<sup>36</sup> A consideration of the broader context is needed to create a holistic picture of the operational environment.

A truly holistic analysis will need to encompass narratives (storylines) in addition to the tabular boxes (cells in a database) typical of linear models. An approach that is holistic in nature is not implemented through simple fact-finding alone, but also by placing these facts in their context, such as time, location and culture or whatever gives the most meaning to the facts. In this respect, some practitioners have distinguished between information (dealing with the 'what'), knowledge (dealing with the 'how') and understanding (dealing with the 'why').<sup>37</sup>

Whereas a linear model is usually based on, and too often ends with, quantifiable data that are fed into the various dimensions, a holistic approach

results in a freer interpretation of the facts.<sup>38</sup> Naturally, interpretations are influenced by the values and beliefs of the analyst.<sup>39</sup> So a key factor for a realistic analysis is the ability of the analyst to grasp the background cultural and historical narrative. As a well-known military anthropologist has noted, it is clear that 'misunderstanding culture at a strategic level can produce policies that exacerbate an insurgency; a lack of cultural knowledge at an operational level can lead to negative public opinion and ignorance of the culture at a tactical level endangers both civilians and troops'.<sup>40</sup>

## Human security intelligence as a model

The aforementioned intelligence models, widely used by NATO intelligence analysts, do not effectively address all dimensions determining 'human security'.<sup>41</sup> The UN Development Programme's (UNDP) highly influential *Human Development Report 1994* introduced the concept to encompass the broader dimensions of security. The factors presented in this original definition of human security are characteristic of a people-centric approach. As shown in Figure 7.2, there is a direct link between the various dimensions of human security. Ignoring one or more of these dimensions can lead to unforeseen risks for the populace as well as the intervening forces and other humanitarian actors.

Therefore an intelligence model needs to be developed to analyse the human security situation within the AOI. The UNDP components of human security are personal security, community security, political security, economic security, food security, health security and environmental security.<sup>42</sup> The model and some examples of the various components are described below.

*Personal security* is freedom from physical violence. According to the *1994 Human Development Report*, in both poor and rich nations, human life is increasingly threatened by sudden and unpredictable violence. The report mentions several forms of threat, including<sup>43</sup>:

- those from the state (physical torture);
- those from other states (war);
- those from other groups of people (ethnic tensions);
- violence between individuals or gangs (crime, street violence);
- violence against women (rape, domestic violence);
- those against children based on their vulnerability and dependence (child abuse);
- violence against the self (suicide, drug use).

*Community security* is freedom from oppressive actions within a community. Specific examples cited by the report include acts of oppression, such as slavery, harsh treatment of women and discrimination, particularly within

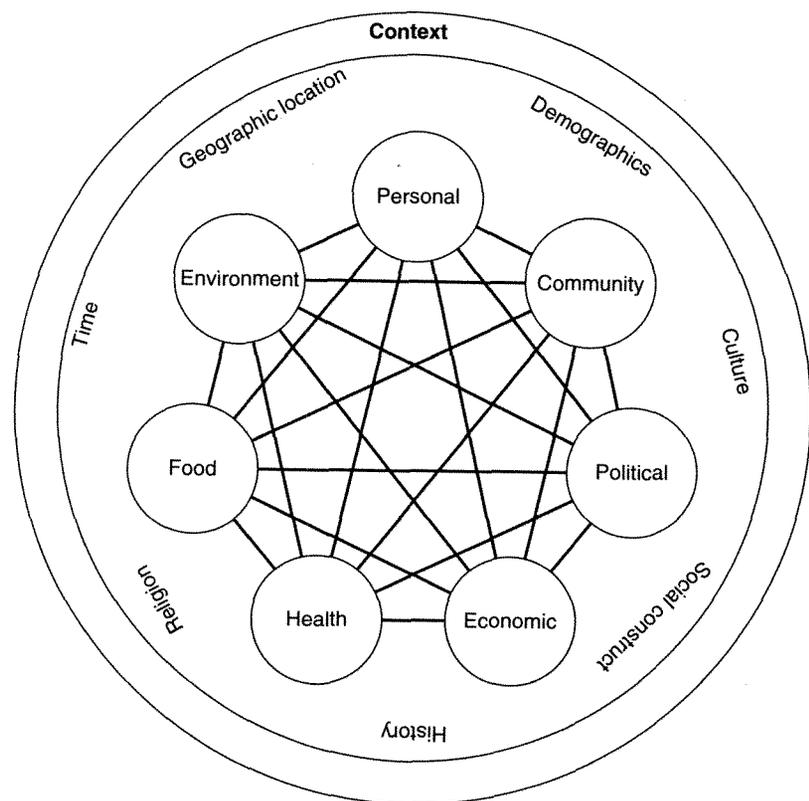


Figure 7.2 Human security intelligence model

more traditional communities. The report also cites the disappearance of traditional languages and cultures as a threat.<sup>44</sup> These practices can culminate in direct threats to personal security – for instance, through tribal wars or ethnic cleansing.

*Political security* is freedom from state repression. The 1994 *Human Development Report* gives the following examples of state repression: political repression, political detention and imprisonment, systematic torture, disappearances, and control of ideas and information.<sup>45</sup>

*Economic security* means, among many things, an assured basic income. Productive and remunerative work, or in the absence thereof a public financial safety provision, is key to economic security.

*Health security* can be measured by human life expectancy, absence of diseases and access to health care.

*Food security* relies on physical and economic access to basic food and water.

*Environmental security* relates to the general condition of the environment and effects of environmental disasters on human lives.

Following the causal pathways depicted in Figure 7.2, personal, community and political security can be regarded as subsets of freedom from fear, while economic, food, health and environmental security are subsets of freedom from want.

Holistic models, which result in a richer understanding of the environment, are more difficult to summarize using acronyms since they are constructed on case-specific combinations of relevant dimensions. Given the fact that human security is a holistic construct, the temptation to create an acronym for the elements of the HSI model is best left unsatisfied.<sup>46</sup> Rather, the various security types outlined by the UNDP should be analysed in their relevant context to give true meaning to their variables. The model emphasises that not only do the variables within the different dimensions matter, but more importantly the causal relationships between the dimensions matter. Furthermore, the aforementioned problem that analysts often do not sufficiently take context into account is addressed by making the context part of the model itself.

Admittedly, the proposed HSI model is a complicated one, creating a multidimensional picture that can be difficult to conceptualise simply. The number of variables influencing the various human security types considered in the model is almost endless. The savvy analyst will have to prioritise the factors that are most pertinent. Given the large number of causal pathways, a true holistic analysis can be conducted in the form of a narrative to complement or replace a database of variables.<sup>47</sup>

The value of the proposed HSI model lies in the fact that it is population-centric or human-centric, and thus more directly related to the desired end state. When properly applied, it could provide valuable intelligence to guide an operation. It can also provide early warnings about possible conflicts to the commander of the PO. For example, in Haiti, food riots were triggered by global commodity prices, something that was not foreseen by the UN mission, whose intelligence efforts were focused on in-country indicators. Using the comprehensive approach afforded by HSI, the commander could have stood a better chance of identifying and addressing the root causes proactively and preventively rather than dealing with the resulting unrest.

Since the HSI model is constructed around the UNDP model, it does, however, not explicitly provide information regarding military and legal aspects which are emphasised in more traditional models. Therefore the model could be used in combination with other operational intelligence models, such as PMESII and ASCOPE.

## Incorporating intelligence sources and OSINT

Having seen what a HSI model might be composed of, and some of its benefits, the next step is to consider how the various sources of information or intelligence can be incorporated into it. In the traditional intelligence literature, a number of collection disciplines or source types are distinguished:

- ACINT (acoustic intelligence): detection and tracking of sound;
- HUMINT (human intelligence): information from human sources (for example, talking or messaging with people);
- IMINT (imagery intelligence): images (still or video), such as photographic, infrared, multispectral, taken from platforms on the ground, in the sky or in space;
- MASINT (measurement and signature intelligence): scientific and technical information to identify equipment (for example, weapons) used in the AOI;
- RADINT (radar intelligence): information gathered by radar systems, for instance, to detect movement;
- SIGINT (signals intelligence), which can be divided into COMINT (communications intelligence) for the detection and tracking of communications from an individual or groups and ELINT (electronic intelligence) to detect and analyse electronic signals other than communications signals in the AOI;
- OSINT (open source intelligence): information available in the public domain, such as Internet, books and newspapers.

The intelligence sources used may be an outcome of both the environment and institutional preferences. For example, in a counterinsurgency operation where the local population may be hostile, as was often the case during NATO's operations in Afghanistan, the military alliance has leaned heavily on traditional means of information gathering, such as SIGINT, IMINT and MASINT. HUMINT is also valuable but sources need to be carefully vetted. Because modern POs tend to occur in HUMINT-rich environments, it is more natural for them to utilize this source. In Haiti, the UN mission went as far as to hire paid informants to gather information about gangs and their leaders to facilitate arrest operations.<sup>48</sup>

More generally, POs can rely heavily on OSINT since the activities of the mission are not secret. In wars and counterinsurgencies, adversaries go to great lengths to hide information from each other. In POs, the environment is more permissive, though not entirely. While OSINT is often the most important source for HSI, information found in open sources will need to be corroborated with information gathered directly in the crisis area, some of which may need to be gathered from secret sources and by secret means.

As explored in the other chapters of this volume, recent developments in IT have had huge impacts on the utility of OSINT. For instance, in Chapter 6, a range of these technologies have found uses in humanitarian contexts. However, the usual caveats regarding misinformation apply. So the savvy intelligence analyst learns how to find the best sources and how to corroborate information across as many sources as possible.

## Gathering information in an exploding OSINT domain

With the information explosion covering many areas of human security, a major problem arises: one can easily drown in the available information. In humanitarian and peace operations, accurate and timely information is paramount for planning, execution and evaluation. The intelligence analyst, sometimes located in the field and sometimes elsewhere entirely, does not have the time to search through endless sources of information. Basic Internet search tools are valuable, but they also lead to large numbers of results that exceed the ability and the willingness of even a dedicated user to look through.<sup>49</sup> More specific search platforms such as Google (Scholar, Books, site-specific searches) and the Internet Archive (Wayback machine) can be powerful aids.

Prior to the establishment of a specific PO, useful information can be found directly on websites of international organisations, NGOs, governments and other organisations already active in the AOI. One problem here is that information can be poorly presented or manipulated. For example, indicators and indices can be, and sometimes actually are, misused by, for instance, aid donors, international investors, and even analysts and academics.<sup>50</sup> Aid donors sometimes exaggerate death tolls or the severity of a given situation for fundraising purposes.<sup>51</sup> The *Human Security Report 2009/2010*, for instance, mentions the excessive death toll estimate of the International Rescue Committee (IRC) of the war in the Democratic Republic of the Congo in the period 1998–2007. The report claims that this estimate was based on questionable methodology.<sup>52</sup> This underscores the conclusion that information from sources should be corroborated by others.

Given the fact that many sources manipulate information for a variety of purposes, just collecting and analysing the information found in open sources is not sufficient. Information about the sources found and used should also be recorded. For example, the ownership of the source, information about possible partisanship, track records regarding accuracy and so on should always be taken into account when information is being used.

For the purpose of monitoring social media such as Twitter, Flickr and Facebook, a growing number of tools are available for the intelligence community. Some of these methods and their implications are discussed elsewhere in this volume. However, a prerequisite for effective and timely OSINT collection, across the board, is the availability of a robust ICT

infrastructure, with a good connection to the Internet and major databases (governmental and non-governmental). This should be borne in mind when intelligence cells are established since connectivity can pose a problem in conflict zones.<sup>53</sup>

### From information to intelligence in the field

In militaries around the world, the processing of information at the brigade level typically takes place in a collation unit where collected information is stored at an all source intelligence cell (ASIC). There military analysts work to analyse and integrate this information in order to produce an assessment of the AOI, thus turning information into intelligence.

The UN has taken a more holistic approach in its operations since 2006: UN POs have a Joint Mission Analysis Centre (JMAC), usually based at the mission headquarters and sometimes at regional offices of the mission, where military, police and civilians work together. However, given that military personnel are much more numerous in peace operations and that military intelligence officers are easier to acquire, the JMACs tend to be mostly military. The JMAC looks at longer-term analysis while a Joint Operations Centre (JOC) looks at the daily intelligence needs of the mission.

The introduction of HSI in the operational environment is likely to cause some problems, especially since analysts will be confronted with much more information relating to many more dimensions than previously. Much of this information will come from the civilian domain, including open sources, but given the multiple causal linkages with the military domain, it must be handled as equally relevant as traditional intelligence. HSI analysis is multidisciplinary, and necessitates the engagement of expertise not routinely present in armed forces' intelligence communities. Therefore ASICs should be augmented with experts in the various domains, who in most cases must be drawn from civilian bodies, such as governmental or academic organisations.

Beside the challenges presented by this novel approach, fresh opportunities also arise, especially relating to new tools. Increasing computer power and new software solutions enable the JMACs, JOCs, ASICs and the intelligence community operating remotely to manipulate available information, visualise dynamics, and recognise patterns and indicators of trends.

Another key problem lies in information management, a key function that is often neglected or overlooked in military operations, since 'neither analysts nor collection managers/specialists want to be "information managers" and therefore responsible for the tedious naming, storing, archiving, organising, cross-referencing and retrieval of information'.<sup>54</sup> Too often information storage is regarded as an IT function, and thus left to the IT staff to deal with.

For example, during the first six rotations of the Task Force Uruzgan in Afghanistan, there was no information-management position within the

intelligence staff.<sup>55</sup> No data-management protocols had been established, with all incoming and produced information stored in an unstructured folder system that was only partially searchable. On top of this, every rotation of the intelligence staff reinvented the entire information folder structure. This led to a situation where the intelligence staff of the seventh rotation of the task force was confronted with a system where the information was buried in an unmanaged and unstructured storage system consisting of over 42,000 folders that went up to 18 layers deep. Despite the presence of a word-search function, a large part of the information remained irretrievable.<sup>56</sup>

The Australian contingent in Task Force Uruzgan used a different organisational approach to collation and analysis. The intelligence cell was composed of a 'front office' that consisted of only two or three officers, whose task was to collect the incoming information and relay it to an intelligence 'back office' in Australia. This Australia-based office was a permanent collation ASIC with staff serving longer than six months, thus gaining the necessary skills and experience for thorough analysis. The back office conducted analysis and collation in Australian databases, and sent intelligence reports to the Australian front office in Afghanistan for further dissemination. This ensured continuity within the workforce where lessons learned were directly fed into the organisation, thus leading to a constantly improving quality of work and intelligence output.<sup>57</sup> Such a model could be equally beneficial for other small armed forces, such as the Dutch and Canadian militaries.

### HSI: Implications, challenges and opportunities

The increasing need for HSI will further increase the importance of OSINT, which is already one of the most important sources of information in complex emergencies. Much of the information for the HSI model can be gleaned from open sources, especially from governmental and non-governmental organisations.

Some NGOs in the field, however, may be reluctant or unwilling to contribute to intelligence cells since they feel that this could seriously jeopardise their neutrality.<sup>58</sup> So intelligence officials must be sensitive when they reach out to cooperate with NGOs.<sup>59</sup> In fact, some intelligence personnel act as 'salesmen', convincing specialists and organisations to cooperate closely with them.<sup>60</sup> Civil-military cooperation (CIMIC) officers can also play an important role to persuade civil organisations and individuals to cooperate. For example, in the Netherlands, CIMIC reserve officers were able to collect large quantities of valuable information for the new police-mentoring mission in the Afghan Kunduz province, mainly from open sources and from Dutch offices of NGOs already present in Kunduz. Ideally, all of the partners in peace operations would train together and adopt an information-sharing model, perhaps across the eight 'tribes' described by Steele (academia,

civil society, commerce, government, law enforcement, media, military and non-government/non-profit personnel).<sup>61</sup>

The constraints provided by organisational cultures may also need to be overcome. For example, on the military side a shift of culture from 'need to know' to a 'dare to share' basis would be welcome. As already stated, civilian organisations in the mission area should be seen as potential new 'clients' for the products of the intelligence staff. As stated earlier, the intelligence community is quite reluctant to share information with these organisations, which are reluctant to share with the intelligence community. NGOs are, generally speaking, more willing to cooperate with the intelligence cell when they can expect something in return – for instance, security assessments or threat warnings, assessments on the fairness of election polls, or other kinds of information.<sup>62</sup> This also means that the introduction of HSI may necessitate a reassessment of classification levels.

Another possibility to fill the expertise gap is currently being examined by the Royal Netherlands Army, where an environment cell is taking the intelligence role. This cell consists of military staff that can be augmented with civilian staff, who have specific expertise that is normally not available within a military intelligence cell, such as economists, development specialists, medical specialists and environment specialists.<sup>63</sup> Local and regional expertise might also be added to this cell. However, civil experts are often reluctant to be sent to high-risk mission areas. Where, at mission level, the analysis component of the intelligence cell is often located at coalition headquarters in safer locations, such as at Supreme Headquarters Allied Powers Europe in Belgium, this reluctance may not play an important role.

Similarly, in Afghanistan, the US also worked to expand the people collecting information, to include anthropologists, as part of its Human Terrain System project. These academics contributed to a better understanding of the deeper cultural, linguistic and societal factors, and shared their insights with US and international forces. However, this caused considerable controversy: the American Anthropological Association, for instance, disapproved of using academics as intelligence-gathers and analysts since the information could be (and likely was) used to help to carry out combat operations against certain indigenous groups.

The use of civilian experts in the field could pose other problems.<sup>64</sup> The Law of Armed Conflict does not recognise these experts as combatants and as such they are not legally protected as a soldier is under the Geneva Conventions. Insurance can also play an important role, with many health insurance policies excluding armed conflict. Some militaries deal with this by including persons with the requisite skills in their reserve forces.<sup>65</sup>

A further organisational solution could be to outsource specific intelligence tasks to military support firms. These are a type of private security company with a number already being active in the field of intelligence.<sup>66</sup> However, these firms work on a commercial basis and working with them

requires contracts and constraints. In the situation of Task Force Uruzgan, a UK military support firm was hired by the Dutch government to operate leased unmanned aerial vehicles (UAVs). The contract provided for a fixed number of flight hours, and the lack of flexibility regarding additional hours potentially led to a loss of valuable information. Also the effectiveness of flight hours was not discussed, which, due to technical problems with the UAVs, led to major expenditures for limited overall effectiveness.<sup>67</sup> Besides this, most military support firms working in the intelligence field are not specialised in the freedom-from-want dimensions of HSI, often being staffed by retired military personnel.

New systems and technologies are finding their way into the intelligence community to support the analysis of the vast quantities of information. Three groups of analytic solutions are being distinguished: information fusion, data-mining and visual analytics.<sup>68</sup> Information fusion methods have been developed to automate the process of detection, classification and prediction of phenomena in various fields. Concurrently, data-mining techniques help to discover identical patterns from a multitude of different sources. Visual analytics are also being used to link and analyse large amounts of data stored in many different databases.<sup>69</sup> As has been shown, there are a multitude of challenges to overcome. Concurrently, there are many exciting and innovative developments which provide ample opportunities for analysts.

## Conclusion

The nature of complex emergencies is multifaceted, especially since armed conflict is involved. Humanitarian and peace operations are undertaken in challenging environments, especially for those involved in the crucial field of information-gathering. This chapter has argued that a single-faceted understanding of any humanitarian situation is insufficient. Military and civilian leaders in POs need to gain a comprehensive understanding of the conflict area. Currently used intelligence models mainly focus on military aspects and are often focused on instruments of national power. They are not fit for purpose to build a comprehensive understanding of the situation from the point of view of the local populace. The proposed HSI model, however, is built around the civil populace. It analyses the diverse threats facing local populations from a large number of different relevant angles, as well as considering the relationships between these threats.

In traditional military operations, OSINT is usually regarded as less important than the directly gathered traditional military intelligence. However, the more permissive environment of peace operations allows for a more active role for OSINT. This paired with the ITC revolution means that OSINT has greater relevance, and POs have more opportunities to harness its power.

For the proposed HSI concept, OSINT can be a major, if not the principle, source of information.

However, the problem with open source information is less the lack of available information and more the overwhelming abundance of it. Looking for timely and accurate information requires efficient searching strategies. Professionals with skills in information-mining can use their training to ask the right questions and use the right search methods, helping to find the best answers. They can evaluate the reliability of sources and use corroboration across sources to verify information.

To analyse the wealth of collected HSI in complex emergencies, military staff need to be augmented by civil experts. Such experts can be drawn from a range of organisations, such as academic bodies, NGOs, governmental organisations and local organisations. However, using such experts does not come without challenges. Reluctance for civil-military cooperation on both sides needs to be overcome, something that should be easier in peacekeeping than in war-fighting. Also, there are a number of difficulties faced by both civilian and military personnel to operationalise joint intelligence efforts in the field.

With the enormous increase in computing power and software, intelligence analysts can expect new solutions to take some of the burden from their shoulders. However, the challenges of organising information-gathering and analysis in hostile environments remain. The value of OSINT, and the need to harness it in HSI, provides a new frontier for information exploration in peace operations. Hopefully this will allow the international community to better deal with complex emergencies in the future.

## Notes

1. This chapter is believed to be the first work to propose and elaborate on the concept of HSI. The only published source that we find to use the term HSI was in conjunction with police operations, using domestic UK examples. See James Sheptycki, 'Policing, Intelligence Theory and the New Human Security Paradigm: Some Lessons from the Field', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence Theory: Key Questions and Debates* (New York: Routledge, 2009), p.166.
2. 'Complex/Manmade Hazards: Complex Emergencies', *International Federation of Red Cross and Red Crescent Societies*, <http://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/definition-of-hazard/complex-emergencies/>.
3. Ibid.
4. NATO uses the term 'peace support operation' (PSO) to describe such operations, while the UN usually uses the more traditional term 'peacekeeping operation' (PKO). The US uses the broader term 'peace operation'. That more encompassing term is also preferred by us.
5. An early and insightful distinction between conventional and emerging threats was offered by General Al Gray, then commandant of the US Marine Corps, in his article 'Global Intelligence Challenges in the 1990's', *American Intelligence Journal* (Winter 1989–1990), pp.37–41. He characterised the emerging threat as non-governmental, non-conventional, dynamic or random, non-linear in its development of force capabilities, without constraints (rules of engagement), with unknown doctrine, no established indications and no warning network that could be monitored, and an unlimited fifth column unknown to conventional counterintelligence organisations.
6. Brad E. O'Neill, *Insurgency & Terrorism: From Revolution to Apocalypse*, Second edition (Washington, DC: Potomac Books, 2005), p.32.
7. Department of National Defence, B-GJ-005-307/FP-030, *Peace Support Operations* (Ottawa, ON: DND Canada, 2002), pp.5–8.
8. Ibid., p.2.
9. Benjamin Perrin, 'Guns for Hire – with Canadian Taxpayer Dollars', *Human Security Bulletin* (2008), Vol. 6, No. 3, p.5, [http://www.redr.org.uk/objects\\_store/security\\_privatization\\_-\\_challenges\\_and\\_opportunities\\_2008\\_.pdf](http://www.redr.org.uk/objects_store/security_privatization_-_challenges_and_opportunities_2008_.pdf).
10. Christopher Spearin, 'What Manley Missed: The Human Security Implications of Private Security in Afghanistan', *Human Security Bulletin* (2008), Vol. 6, No. 3, p.8, [http://www.redr.org.uk/objects\\_store/security\\_privatization\\_-\\_challenges\\_and\\_opportunities\\_2008\\_.pdf](http://www.redr.org.uk/objects_store/security_privatization_-_challenges_and_opportunities_2008_.pdf).
11. Ibid.
12. Department of National Defence, B-GJ-005-307/FP-030, *Peace Support Operations*, pp.5–8.
13. Humanitarian Policy Group, *HPG Research Report, Resetting the Rules of Engagement, Trends and Issues in Military-Humanitarian Relations* (London: HPG, 2006), p.22.
14. Department of National Defence, B-GJ-005-200/FP-000, *Joint Intelligence Doctrine* (Ottawa, ON: DND Canada, 2003), pp.1–4.
15. Major Rob Sentse (RNLA), 'Influencing the Human Terrain. Market Your Product' (2010), <http://www.scribd.com/doc/168500960/Influence-Behaviour-Market-Your-Product>.
16. Major Rob Sentse (RNLA), 'The African Boulevard of Broken Dreams', *American Intelligence Journal* (2012), Vol. 30, No. 1, p.21. <http://www.scribd.com/doc/132071791/The-African-Boulevard-of-Broken-Dreams-American-Intelligence-Journal-Volume-30-2012>.
17. Ibid.
18. Ideally the COP should be common to all actors in the PO. However, in reality this is not the case, since many organisations still pursue their own goals and sometimes refuse to fully cooperate and share information with other actors. For instance, the International Committee of the Red Cross (ICRC) in many cases abstains from close cooperation with any military force in the AOR, even with the forces conducting the PO since the ICRC does not want to compromise its neutrality. Nowadays the COP is mostly common to just contributing military forces.
19. The AOI is often larger than the AOR, since events in neighboring areas often influence the state of affairs in the AOR.
20. Figure 7.1 is based on information found in Pauline Kerr, 'Human Security', in Alan Collins (ed.), *Contemporary Security Studies* (New York: Oxford University Press, 2006), p.99.
21. The HSI model was developed by Fred Bruls, under the supervision of Dr Dorn, as part of a thesis for the Master in Defence Studies programme at the Canadian Forces College in 2011. The thesis is published at [http://www.walterdorn.org/pdf/HumanSecurityIntell-PSO\\_Bruls\\_MDS-Paper\\_ForPublicRelease\\_Feb2012.pdf](http://www.walterdorn.org/pdf/HumanSecurityIntell-PSO_Bruls_MDS-Paper_ForPublicRelease_Feb2012.pdf). For

- the UN report in question, see UNDP, *Human Development Report 1994* (New York: Oxford University Press, 1994), p.24.
22. The craft of intelligence does appear to be evolving more rapidly than in the past. The concept of HSI – an outcome to be sought – should be distinguished from the concept of full-spectrum human intelligence (the sources) as outlined by Robert David Steele in his monograph, *Human Intelligence: All Humans, All Minds, All the Time* (Carlisle, PA: Strategic Studies Institute, 2010).
  23. Col. Jack D. Kem, 'Understanding the Operational Environment: The Expansion of DIME', *Military Intelligence* (2007), Vol. 33, No. 2, p.1.
  24. Acronyms: DIME (diplomatic, information, military and economic); DIMEFIL (diplomatic, information, military, economic, financial, intelligence and law enforcement); ASCOPR (areas, structures, capabilities, organizations, people and events); and PMESII (political, military, economic, social, information and infrastructure).
  25. Personal conversation between one of the authors (Bruls) and LTC Martien Hagoort, staff officer at the Netherlands Military Intelligence School, 17 August 2011. LTC Hagoort explained that DIME and DIMEFIL are not being used on the operational and tactical levels of POs. The only models to be found today are ASCOPE and PMESII. Therefore the Netherlands Military Intelligence School does not train its students in models such as DIME or DIMEFIL. Consequently these models are not discussed in this chapter.
  26. United States Center for Army Lessons Learned, *Handbook 10–41: Assessment and Measures of Effectiveness in Stability Ops: Tactics, Techniques and Procedures* (Fort Leavenworth: Combined Arms Center (CAC), 2010), p.6.
  27. Explanation of dimensions paraphrased from Kem. 'Understanding the Operational Environment: The Expansion of DIME', p.4. The article gives an explanation of both old and recent models, including DIME, DIMEFIL, MIDLIFE, PMESII and ASCOPE.
  28. See US Army, *Field Manual 3-0: Operations* (Washington, DC, 2008).
  29. PMESII was originally meant to analyse the instruments of power that an opposing party possessed and which of these instruments this party was likely to use. This analysis was combined with an estimate of the optimum mix of instruments to be used to coerce this party to comply with the demands of the host nation where the analysis was made.
  30. Personal conversation between one of the authors (Bruls) and LTC Martien Hagoort on 17 August 2011. L. T. C. Hagoort explained that PMESII is the only model that is being taught at the Netherlands Military Intelligence School. However, he opposes overreliance on a single intelligence model, given the risk of tunnel vision. He therefore would like to see ASCOPE return to the syllabus.
  31. United States Center for Army Lessons Learned, *Handbook 10–41: Assessment and Measures of Effectiveness in Stability Ops*, p.6.
  32. Kem, 'Understanding the Operational Environment', p.6.
  33. *Ibid.*
  34. Maj. Brian M. Ducote, *Challenging the Application of PMESII-PT in a Complex Environment* (Fort Leavenworth: United States Army Command and General Staff College, 2010), p.10.
  35. US Army, *Field Manual 3-0: Operations*, pp.1–5; Ducote, *Challenging the Application of PMESII-PT in a Complex Environment*, p.7.
  36. Ducote, *Challenging the Application of PMESII-PT in a Complex Environment*, p.20.
  37. *Ibid.*, p.20, p.53, p.38.
  38. Personal observation by one of the authors (Bruls) in the position of Information Manager of the G2 branch within Task Force Uruzgan from August 2009 to February 2010.
  39. Ducote, *Challenging the Application of PMESII-PT in a Complex Environment*, p.39.
  40. Montgomery McFate, 'The Military Utility of Understanding Adversary Culture', *Joint Forces Quarterly* (2005), No. 38, p.44. Although cultural could be considered to be part of the 'social' dimension of the PMESII(-PT) model, McFate argues that cultural knowledge is often lacking. Culture is certainly not sufficiently taken into account in the application of the PMESII(-PT) model.
  41. The term 'human security' is a debated one. The narrow definition is freedom of individual human beings from physical threats. The broader definition includes all manner of threats (for example, to health, food sources, finances, stability and identity). The masters thesis mentioned in note 21 contains a description of the most important approaches to define the term. See [http://www.walterdorn.org/pdf/HumanSecurityIntel-PSO\\_Bruls\\_MDS-Paper\\_ForPublicRelease\\_Feb2012.pdf](http://www.walterdorn.org/pdf/HumanSecurityIntel-PSO_Bruls_MDS-Paper_ForPublicRelease_Feb2012.pdf).
  42. UNDP, *Human Development Report 1994* (New York: Oxford University Press, 1994), p.24.
  43. *Ibid.*, p.30.
  44. *Ibid.*, pp.31–32.
  45. *Ibid.*, pp.32–33.
  46. It is tempting to designate this model with an acronym referring to the factors that it covers, as do the other intelligence models discussed in this chapter (such as ASCOPE and PMESSI). However, avoiding an acronym has benefits. As shown above, intelligence models in today's operations are often used as a simple exercise of quantifiable fact-finding to feed into different dimensions, while the links between the dimensions are often ignored, leading to information with limited value.
  47. Ducote, *Challenging the Application of PMESII-PT in a Complex Environment*, p.53.
  48. A. Walter Dorn, 'Intelligence-led Peacekeeping: The United Nations Stabilization Mission in Haiti (MINUSTAH), 2006–07', *Intelligence and National Security* (2009), Vol. 24, No. 6, pp.805–835.
  49. Anthony Olcott, *Open Source Intelligence in a Networked World* (New York: The Continuum International Publishing Group, 2012), p.109.
  50. Nada J. Pavlovic, Lisa Casagrande Hoshino, David R. Mandel and A. Walter Dorn, *Indicators and Indices of Conflict and Security: A Review and Classification of Open-Source Data, Technical Report, Defence Research and Development Canada*, Toronto, September 2008, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA494833>, p.3.
  51. Human Security Report Project, *Human Security Report 2009/2010: The Causes of Peace and the Shrinking Cost of War* (New York/Oxford: Oxford University Press, 2011), p.126.
  52. *Ibid.*, p.124.
  53. In many military operations, as in Afghanistan and Iraq, connections were established over narrowband satellite connections. Access to the Internet was very slow, making the search for information from open sources an extremely time-consuming exercise.
  54. Arpad Palfy, 'Intelligence Information Management in Joint Environments', *Vanguard*, December 2010/January 2011, <http://vanguardcanada.com/intelligence-information-management-in-joint-environments/>

55. In order to adopt information management as a topic in the curriculum of intelligence personnel, in 2010 a working group was established at the Netherlands Military Intelligence School in which one of the authors (Bruls) plays an advisory role.
56. Personal observation in the position of Information Manager of the G2 branch within Task Force Uruzgan from August 2009 to February 2010.
57. Personal conversations with the MRTF S2 and Australian liaison officers within the ASIC within the G2 branch within Task Force Uruzgan over the period August 2009 to February 2010.
58. Ibid.
59. MGen Michael T. Flynn, Capt. Matt Pottinger and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for a New American Society, January 2010), [http://www.cnas.org/files/documents/publications/AfghanIntel\\_Flynn\\_Jan2010\\_code507\\_voices.pdf](http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf), p.9.
60. See Adam B. Siegel, 'Intelligence Challenges of Civil-Military Operation', *Military Review* (September/October 2001), pp.45-52.
61. Robert David Steele, 'Information Peacekeeping and the Future of Intelligence: The United Nations, Smart Mobs and the Seven Tribes', in Ben de Jong, Wies Platje and Robert David Steele (eds.), *Peacekeeping Intelligence: Emerging Concepts for the Future* (Oakton, VA: OSS International Press, 2003), pp.201-255.
62. Ibid.
63. Royal Netherlands Army, *Command Support in Land Operations: Doctrine Publication 3.2.2.1. Study Draft 4 (CONCEPT)*. pp.6-19. Special thanks to LTC Chris Rump, RNLA for providing us with this draft.
64. McKinsey, *Big Data, Small Wars, Local Insights*, <http://voices.mckinseysociety.com/big-data-small-wars-local-insights-designing-for-development-with-conflict-affected-communities/> (accessed 1 May 2013).
65. See Siegel, 'Intelligence Challenges of Civil-Military Operation'.
66. For an overview, see Victoria Wheeler and Adele Harmer (eds.), *Resetting the Rules of Engagement, Trends and Issues in Military-Humanitarian Relations* (London: Humanitarian Policy Group, March 2006), <http://www.odi.org.uk/sites/odi.org.uk/files/odi-assets/publications-opinion-files/273.pdf>, p.68.
67. Personal observation by one of the authors (Bruls) in the position of Information Manager of the G2 branch within Task Force Uruzgan from August 2009 to February 2010.
68. Gregor Pavlin, Thomas Quillinan, Franck Mignet and Patrick de Oude, 'Exploiting Intelligence for National Security', in Babak Akhgar and Simeon Yates (eds.), *Strategic Intelligence Management* (Waltham, MA: Butterworth-Heinemann, 2013), p.167.
69. Ibid., p.186.