Community of Intelligence: The Secret Behind Intelligence-Led Policing

Mariëlle den Hengst
Systems Engineering, Delft University of Technology
Lectureship Intelligence, Police Academye
the Netherlands
marielle.den.hengst@politieacademie.nl

Jan ter Mors
National Intelligence Program
Dutch Police Force
the Netherlands
jan.ter.mors@vtsn.politie.nl

Abstract— Intelligence-led policing is the use of analyzed information by decision makers to decide on police resources. Analysis is very important in this and increasingly needs to be a collaborative effort: tools, techniques and the complexity of crimes far exceeds the capacity and expertise of any single analyst. Analysts have to collaborate to create an understanding. In this paper we describe how the Dutch police force has built a community of intelligence in which analysts can collaborate to create intelligence reports for intelligence-led policing.

Keywords— intelligence-led policing; intelligence analysis; community of practice

I. INTRODUCTION

Intelligence has been recognized as being important in policing since very long. Most commonly, intelligence is seen as the information gleaned from various sources (secret intelligence agents) on the activities of known or suspected active criminals. Since the 1990s several drivers caused the intelligence to be viewed as more, starting in the United Kingdom. One driver was the newly created knowledge that most crimes were committed by a small number of offenders [1]. By targeting on the criminal instead of the crime, the police would be able to be proactive and prevent crimes to happen. Another driver was the increasing workload and, as a result of this, the increasing need to decide on how, where and when to use police resources as to combat crime as efficiently and effectively as possible. For both drivers, the police are in urgent need for information on patterns in criminal activities, series of crimes, hot spots, and opportunities for criminal activities. And this information need is not restricted to “secret intelligence” but can be based on all sorts of intelligence collected from incident data, community information and information from partners in the security domain.

The huge security issues are another driver for the increasing importance of intelligence in its broad sense. In recent years, a number of major events (the 9/11 attack, the bombings in London and Madrid, the disastrous dance parade in the Netherlands in 2009, the love parade disaster in Duisburg in 2010 and the riots in the summer of 2011 in Great Britain) show that the intelligence process has failed [2, 3]. Internally and internationally nation states face security challenges arising from terrorism and organized crime and also in the area of public order management. National and international security and police organizations have increasingly devoted substantial resources to gathering and analyzing intelligence to try to combat these challenges. Intelligence-led policing (ILP) has been largely embraced for this [4]. ILP can be defined as the use of analyzed information and knowledge by decision makers to decide on police resources. With ILP, not only is intelligence needed for evidence to prosecute crimes, it is also needed to make an analysis of all sorts of information to predict crimes and to proactively and objectively direct police resource decisions [4].

Intelligence-led policing has an international resonance whether in the United Kingdom, the United States of America, Australia or in the Netherlands. By 2002, the New Zealand Police were committed to intelligence-based policing. In the USA, the International Association of Chiefs of Police called for a national policing plan to promote intelligence-led policing in 2002. By 2003, every police service in Australia had reference to intelligence-led policing. In the UK, all forces have adopted the National Intelligence Model by April 2004. The Board of Police Commissioners in the Netherlands decided upon the Dutch National Intelligence Model by 2008.

In many instances of ILP great emphasis is placed on the analysis part of ILP: tools are being developed to support ever increasingly sophisticated analysis techniques, technologies are developed to use the ever increasing amount of information available, mostly through internet and social media, and training programs for analysts have never been so popular [5]. These developments all focus on improving the working conditions for the individual analysts, in the hope that this would result in policing better led by intelligence. Today’s society, however, is characterized by increasing volumes of information, an increasing complexity of criminal phenomena, fast developing technologies and techniques. Digesting, processing and interpreting this information to make sense of crimes with constantly developing methods and techniques far exceeds the capacity and expertise of any single analyst [6-10]. Integration and collaboration is needed to ‘produce the best intelligence available’.

Integration and collaboration is about sharing information, sharing knowledge and sharing expertise. Integration and collaboration do not happen by itself, or as a result of mentioning it in strategic documents and plans. A working environment is needed which supports and
promotes a culture of information sharing and collaboration. A community of practice is such a working environment that supports this sharing. A community of practice is a group of people who share a profession and in which the members learn from each other through the process of sharing information and knowledge [11]. Communities of practice can exist online, like in discussion boards and newsgroups, or in real life, such as in a lunchroom. To support the collaboration of analysts in intelligence-led policing, Sprenger et al. [12] therefore propose a community of intelligence. A community of intelligence relies on the mechanisms of a community of practice and has intelligence as binding content.

Just as integration and collaboration do not happen merely because it is written down in some strategic documents, a community of intelligence will not arise because some people believe in it as a solution for lack of collaboration. Building a community of intelligence requires great efforts, continuing enthusiasm and long-lasting energy. But, once realized, a community of intelligence is the secret behind intelligence-led policing, allowing for the best intelligence to be produced. Although a lot of research and literature is available on how to realize a successful community of practice in general, hardly any of this literature focuses on the specific characteristics of an intelligence community in the security domain. We performed a case study to learn about the specific needs for a community of intelligence in the security domain. The case which we used for our action research is that of the community of intelligence in the Netherlands. The Dutch police started to implement a community of intelligence in the summer of 2010 as part of the implementation of the National Intelligence Model. Now, almost two years later, the community has grown to a group of over 535 analysts, which contribute to the success of intelligence-led policing. This paper presents the lessons learned when building the community of intelligence and the secrets of the community of intelligence for intelligence-led policing.

In this paper, we first present background information on intelligence-led policing, the implementation of intelligence-led policing in the Netherlands and the experiences with communities of intelligence worldwide. The research method used is described in the third section. In the fourth section we then focus on the process of the realization of the community of intelligence in the Netherlands. We describe the power of the community of intelligence in the fifth section. And we conclude this paper with recommendations for further realization of the community of intelligence.

II. BACKGROUND

A. Intelligence-led policing in the Netherlands

The concept of intelligence-led policing has gained a lot of attention in the past decade or so, resulting in the implementation in several countries around the world. Although the concept of intelligence-led policing is similar in the various developments worldwide, the implementation of the concept into practice varies between the countries and even within the countries: varying quality of intelligence reports, different standardized formats or a lack of standardization, differences in the number of analysts working for the intelligence process, and different levels of education for the analysts [13]. It is difficult to define intelligence-led policing precisely [14]. So we will not try to do so, but we will describe some of the important elements that together constitute intelligence-led policing.

Intelligence-led policing is about information. Although intelligence might by some people still be linked to ‘secret intelligence’, a much broader set of information sources together constitutes intelligence nowadays. To some people it is all information and knowledge that is available, including for example the financial state of a unit or the state of maintenance of patrol cars [14]. To others it is limited to criminal and crime related information. When policing is about security, intelligence should enable to make sense of the security issues that have to be dealt with. Then, information should not be restricted to criminals and crimes only.

Intelligence-led policing is about the analysis of this information. Different people give a different meaning to analysis. Some people state that in order to speak of analysis you need to apply some formal method or tool to the information to create intelligence or significant information. Others state that even the ‘simple’ determination that information is significant is a form of analysis [15].

Intelligence-led policing is about the knowledge and behavior to use this analyzed information by decision makers. Intelligence is only as good as the use made of it [16]. Vital to the success of intelligence-led policing is that intelligence influences the thinking of the decision makers [17]. This might sound simple in theory, in practice it is pretty hard to realize. First, because decision makers in the police are not used to being advised, and especially not to being advised by analysts that, more often than not, are civilians. Intelligence, historically, was limited to reactive analysis of events after they had occurred. Pro-actively being advised before a decision is being made does not have such a long history. And it takes quite some effort for decision makers to set their intuition and feeling about a certain security problem aside and to rely on the information provided by the analyst, even if this contradicts their initial beliefs [18]. Decision makers need knowledge to understand the analytical product and need the right behavior to really use this understanding to make decisions. Furthermore, analysts need good interpersonal skills to really influence decision makers [19]. In the enrollment of analysts, analytical skills are emphasized far more than interpersonal skills.

Intelligence-led policing is about the use of this analyzed information and knowledge by decision makers to decide on police resources. This is not restricted to investigative resources only. Public order management, surveillance and emergency response benefit from intelligence-led decisions about the employment of police resources at least as much as investigation does.

Inspired by the developments in the UK concerning intelligence-led policing, Dutch police forces started to give intelligence-led policing meaning by the beginning of this
B. Communities of intelligence

A community of practice is defined as a group of people who share the same interest and who interact regularly in order to learn from each other [23]. Establishing discussions should be one of the main functions of a community because it is a means to expand knowledge [24]. While the original concept of communities of practice is based on face-to-face interaction, the advancement in information and communication technology has widened this concept as space and time barriers collapsed. This increases the prominence of communities of practice and at the same time creates new challenges in building and sustaining communities of practice. Virtual environments increase interaction barriers that hinder effective coordination and communication [25]. It makes people less attentive and less receptive to contextual cues [26] and hinder the creation of trust [27]. A secure environment is needed for people to feel free to share knowledge [28]. And people also need to be motivated to share knowledge [29]. For some people this motivation comes from the altruistic feeling of helping someone with information, but most people need an external form of motivation for this [30]. A reward in the form of a recommendation system [31] or in the form of being helped with the information shared through the community are examples of potential motivators. Virtual environments, furthermore, enable large numbers of people to join the community. This endangers the sense of identity and members’ commitment toward the community [32]. A clear objective of the community is needed to prevent this as well as a close relationship with the actual work of the members [33]. Key issue for sustaining a community of practice is maintaining the participation of members [34]. Continuous stimuli by starting new discussions and by providing contradicting viewpoints in existing topics keeps participants curious enough to return to the community of practice [32].

Above described mechanisms are true for ‘average’ communities in business and education settings and from those studied in laboratory research. Intelligence communities, however, differ systematically from those types of communities [35]. First, intelligence professionals work with incomplete, imprecise and contradictory information and constantly face adversaries who attempt to conceal or manipulate information [36]. Intelligence professionals perceive intense pressure since they deal with considerable security issues [36]. This pressure is intensified in today’s society where wrong intelligence is seen and treated as a failure of policing. And most importantly, information sharing, although promoted, is not in the backbone of the intelligence professional that often deal with secret and vulnerable information. These differences may make intelligence communities particularly susceptible or resistant to common measures to build and sustain communities of practice. Important for a sustainable community of intelligence are collective training, a reward structure that recognizes collaboration over individual performance, joint projects, personal interactions in casual settings to develop trust and a virtual platform for knowledge sharing, through discussions and finished products [10]. The steps we have taken as part of the case study to overcome the resistance are presented in the next section. Below we describe some successful examples of communities of intelligence elsewhere in the world.
In the aftermath of the tragedy of September 11th, 2001, the momentum for changing how the US intelligence community does its business became irresistible. Regardless of the improvements established, the consequences were only marginal [6]. By the end of 2007 a new strategy was agreed upon: ‘to transform the analytic component of our community from a federation of agencies, or a collection of feudal baronies, into a community of analysts’ [37]. Several initiatives have been implemented to support this community of analysts in the US. First, for analysts to collaborate, they must be able to locate one another. Simple in its form, but a insuperable impediment to collaboration, was the introduction of the Analysts Yellow Pages [6]. One of the most vital initiatives was that of joint training [6]. Analysts would get to the same quality level, would speak the same language and would get to know each other, key to develop trust for sharing information and collaboration. An evaluation process was set up to regularly review finished intelligence products and to feed back these results to training units, to directors of analysis and in workshops. These evaluations have become instruments for continuous improvement of the intelligence community. A Library of National Intelligence (LNI) was created which contains fully sourced versions of all finished intelligence products. In little more than a year, the LNI counted some 800,000 products and was adding some 20,000 products each week [6]. Whereas joint training is the front-end of the production cycle of intelligence, LNI is the back-end. In between is the analytic process itself, where collaboration is most vital and most difficult. A classified social networking site was developed for this purpose, A-Space [6]. A-Space offers analysts the opportunity to brainstorm as they develop their thinking and share rough drafts for comments of their peers [38].

A-Space is dedicated to the US Intelligence community. Communities that have a broader focus are, for example, the International Association of Crime Analysts (IACA: www.iaca.net) and the International Association of Law Enforcement Intelligence Analysts (IALEIA: www.ialeia.org). Both associations aim to improve the professionalism in intelligence analysis all over the world. They do so by providing training, offering networking events, setting standards, offering certification programs and publications. Although these kinds of communities contribute to the professionalism of intelligence analysis in general, they do not offer a secure environment to collaborate on specific analytical assignments, as A-Space does. For the Dutch police a community is needed that supports the collaboration in working on complex analytical issues as well. In the fourth section, we describe the steps we have set to create a community of intelligence for the Dutch police as part of the case study, which is described in the next section.

III. RESEARCH METHOD

This paper reports on lessons learned regarding the successful realization of a community of practice in the security intelligence domain. The case study followed an action research approach. Action research has the dual intention of improving the practice and contributing to theory and knowledge [39, 40]. Action research was considered appropriate for several reasons. First, the phenomena at hand were considered too complex to be studied in a constructed setting. Second, action research is especially appropriate to address ‘how to’ questions. Our central research question is ‘how to successfully realize a community of practice in a security intelligence domain’.

We employed the model proposed by Zuber-Skerrit [41], that states that an action research study may consist of four activities that can be carried out over several iterations. ‘Plan’ concerns exploration of the research site and the preparation of the intervention. In this activity, the researchers define the problem to be addressed, both practically and scientifically; both are described in the previous sections. ‘Act’ refers to the actual intervention made by the researcher. This is based on the planned intervention, which may also be informed by starting theories. The interventions are described in the next section. ‘Observe’ concerns the collection of data during and after the actual intervention to enable evaluation. Finally, the ‘reflect’ activity analyzes the collected data and infers conclusions that may feed into the ‘plan’ activity of a new iteration. Observations and conclusions are presented in the fifth and sixth section.

IV. TOWARDS A COMMUNITY OF INTELLIGENCE

A community of intelligence will not exist just by providing a secure virtual space where members of the community can meet. It will also not just exist by scheduling face-to-face meetings for the members of the community. Well thought steps have been taken to come to a successful community of intelligence. Without getting lost in details, we provide an overview of the steps we have taken.

We started off in June 2010 with a brainstorm with a small group of potential members of the community of intelligence. Purpose of the brainstorm was to detect requirements for a community of intelligence to get started and to identify barriers for this. For the meeting, we invited nine analysts, highly educated, young of age and relatively new to the police. We selected these analysts to start with for several reasons. Because they are relatively new to the police, they are not yet ‘indoctrinated’ by the police culture; they are open to new ways of working and are willing to try these out. And, as they are young of age, they are probably used to not only collaborate in face-to-face settings but also through all kinds of social media on the internet. We used this group of analysts as a focus group throughout the entire process. The brainstorm resulted in the following aspects as must-haves: the possibility to share analytical products and provide feedback on these, the possibility to share methods and techniques, and the possibility to share good practices. They want this through newsletters, twitter-like interaction, RSS-feeds and a database that allows quick access to the right content. One thing that should be guarded for is that police managers and supervisors might feel the urge to give assignments for analysis through the community; the purpose of the community is that peers collaborate to improve their analytical work. The most important barriers indicated by the
analysts are that sharing information is not common, not within a single police force, let alone between the 26 different police forces the Dutch police counted at that time. Another important barrier is the fact that for sharing analytical products, analysts more often than not need permission from their superior. Finally, technical impediments might prohibit the use of a community of intelligence. Most of the features for virtual communities available through the internet cannot be used by the Dutch police because of several security restrictions. And those that may be used require a laborious procedure to be used.

In addition to this enquiry of needs and requirements, we used an electronic questionnaire that was sent to representatives of all 26 Dutch police forces with the request to spread it out to the analysts working in their force. This resulted in a response of 45 analysts filling in the questionnaire during the summer of 2010. About half of the respondents foresees to visit the community between 10 and 30 minutes weekly, whereas 31% of the respondents would visit the community for even up to 60 minutes. Around 20% of the respondents does not yet know whether they will visit the community. No one indicated that they would not collaborate through the community. The needs identified in the questionnaire are similar to the ones identified in the brainstorm. New to this is that the analysts do not want the community to be too informal. They also place more emphasis on the analytical work they do and the knowledge and tools they need for this than that they want the community to contribute to their social network.

During the autumn of 2010 we started the technological implementation of the community of intelligence. We translated the needs and barriers identified into functional requirements. Technical developers used these requirements to realize a virtual community of intelligence through Microsoft Sharepoint 2007. Some of the functionalities could not be implemented, partly because these functionalities are not offered by Sharepoint 2007 and partly because these functionalities are switched off within the Dutch police environment. Examples of functionalities that could not be implemented are a strong search-engine for the community, as well as some sort of recommendation system to reward members of the community for their contributions. Upgrading to Microsoft Sharepoint 2010 might solve some of these problems. However, several reasons exist why this upgrade is not foreseeable in the near future for the Dutch police.

In the winter of 2010/2011 the focus group of nine analysts was invited to participate in the virtual meeting space as it was implemented in Sharepoint. The purpose of this activity was to not only technologically implement a virtual meeting space, but also to generate some first content in the community of intelligence. When content is already present, members of the community might find added value already during their first visit. And the barrier to add content to the community is lowered, since members can use the content already available as an example of what and how to share information. During this exercise, not only content was added to the virtual meeting space, also the look and feel of the meeting space was adjusted to the needs of the focus group.

In the spring of 2011, May 10th, the virtual meeting space for the community of intelligence went on-line for all intelligence professionals working at the Dutch police force as well as for partners in security, such as analysts working for the Public Prosecutor and customs. A nation wide meeting was organized to introduce the community of intelligence on the one hand and to collaborate on the topics that are part of the National Intelligence Calendar. This would provide input for the Dutch police and at the same time generate content that can be shared through the community of intelligence. The participants of this nation wide meeting were added as members to the community of intelligence, resulting in just over 300 new members. Although the community is open to all security intelligence professionals in the Netherlands, they do have to enroll as member to start using the community of intelligence. This enrollment procedure supports the feeling of a safe and secure environment to publish analytical work, to collaborate and to share ideas and knowledge.

Since the formal start of the community of intelligence in the spring of 2011, all efforts are focused on sustaining the community of intelligence. A monthly update of the content of the community of intelligence is sent out to all members by email. An increase in the number of visits to the community of intelligence is visible directly following this monthly email digest. The focus group has been consulted several times to discuss possibilities to further improve the community of intelligence; and they have been interviewed to address the power of the community as described in the next section. Physical meetings for the analytical intelligence professionals are scheduled for; a community is not only a virtual meeting space but also needs physical meetings to build trust and relationships between members of the community. This has resulted in a community of intelligence that, by the beginning of March 2012, counts 535 members. The Dutch police forces together count approximately 50.000 employees of which almost 2.700 are part of the intelligence unit [43]. The community of intelligence is not interesting to everyone in the intelligence unit; supporting staff, for example, might not be interested. Approximately 1500 employees in the intelligence unit, given their daily work, might potentially be interested. From this we can conclude that around 30% of all potentially interested intelligence professionals is member of the community of intelligence. Although this is a wonderful result, the power of the community of intelligence is more than the number of members. We describe this in the next section.

V. THE POWER OF THE COMMUNITY OF INTELLIGENCE

Within a year of time, the community of intelligence has grown from nothing to a large group of intelligence professionals in the security domain. The first 300 members enrolled as a result of participating in a nation wide meeting where the community of intelligence was introduced. The next 235 members enrolled on personal interest to be part of the community. And the number is still growing. As in all social media, such as twitter, youtube, facebook and flickr,
the number of members should be differentiated. The 1%-rule tells us that not all members will be similar active participants to the community of intelligence [44]. Some people enroll a community, but never participate in it; these are inactive members. Most people enroll a community only for the purpose of absorbing the content (90% of the members is assumed to do so). As much as 9% of the members would actively participate in the community by not only viewing content, but also contributing to discussions and editing and modifying content. Only 1% of the active members would also create content, start up new discussions and feed the community with new content. More important however that comparing these figures with those of social media like YouTube and Flickr would be to compare these with other professional communities. For this study we identified one successful professional community within the police and one outside the police and interviewed the moderators. For selecting the successful community within the police, we asked several people to mention a successful community. The network of transport controllers within the police was selected as successful. This is a community of 300 police officers which exists since the beginning of 2010. This makes it successful in the eyes of many, the moderator, however, is not satisfied. There is hardly any activity in the community, all activity is initiated by the moderator itself. The community is considered more or less a database with procedures, rules and legislation concerning transport control, rather than it is an environment where knowledge is created. For selecting a successful professional community outside the police, we selected a community in the public sector, Ambtenaar2.0. This community is for all people working in the public sector, exists since 2001 and has almost 7000 members. A small part of these members is working in the public sector, exists since 2001 and has almost 7000 members. A small part of these members is really active and posts contributions, but this group is large enough to keep the community ‘alive’. Process related issues appear to be shared through the community more easily than content related issues, while the true key to success of a community is when it seamlessly integrates with normal work, so content related. A point of continuous attention is the preference for public organization to organize hierarchically, resulting in managers wanting to take over the control of this non-hierarchical community.

When we relate these lessons and figures to the community of intelligence, the community can be considered a success. Over the past months we have on average 150 unique visits each month. See the figure below for a monthly overview of the number of unique visits. In total, we have almost 1700 unique visits. We have 129 members account for these visits through a police computer and another 99 visits through the internet. Only in case of the use of a police computer to enter the community, can we track down the individual member. In case of internet being used to enter the community, the system does not log the results to an individual member. Because of this, it is impossible to extract the exact number of inactive users; it is somewhere between 58% and 76% of the total number of members. Of the 129 (24%) active users who use the community through the police network, we do have some figures.

Most active members visit the community more than once. The table below presents the percentage of members that visited the community a certain number of times since the beginning of the community. Notice that this does not include the visits through internet: the members that visited the community only once, might have visited the community more frequently through the internet.

<table>
<thead>
<tr>
<th>Number of visits per member</th>
<th>Percentage of active members (129)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No more than 1 visit</td>
<td>12%</td>
</tr>
<tr>
<td>Between 1 and 5 visits</td>
<td>24%</td>
</tr>
<tr>
<td>Between 5 and 10 visits</td>
<td>23%</td>
</tr>
<tr>
<td>Between 10 and 20 visits</td>
<td>20%</td>
</tr>
<tr>
<td>More than 20 visits</td>
<td>20%</td>
</tr>
</tbody>
</table>

Not all members that visit the community also contribute content to the community. Some members only visit the community to absorb the content. The table below presents the percentage of active members (that entered the community through the police network) that contributed one or more items to the community, being it participating in discussions, uploading documents or posting questions.

<table>
<thead>
<tr>
<th>Number of contributions per member</th>
<th>Percentage of active members (129)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero contributions</td>
<td>36%</td>
</tr>
<tr>
<td>Only 1 contribution</td>
<td>19%</td>
</tr>
<tr>
<td>Between 1 and 5 contributions</td>
<td>26%</td>
</tr>
<tr>
<td>Between 5 and 10 contributions</td>
<td>10%</td>
</tr>
<tr>
<td>Between 10 and 20 contributions</td>
<td>2%</td>
</tr>
<tr>
<td>More than 20 contributions</td>
<td>6%</td>
</tr>
</tbody>
</table>

The time spent at the community each visit is on average 9 minutes and 52 seconds, with a minimum of half a minute and a maximum of 53 minutes and 31 seconds.

Taking a closer look at the power of the community of intelligence, several things attract attention. First, analysts appreciate the large network of analysts that they can reach out to through the community. Without a lot of effort, they reach peers in other police forces and other organizations such as the public prosecutor. Without the community of intelligence, they would be in contact with their direct colleagues and with only a few analysts outside their own department, whom they got acquainted with through training.
or seminars. The community of intelligence gives them easy access to greater amounts of knowledge and experiences.

Second, the community of intelligence increases analysts’ situational awareness. Through discussions and documents posted, analysts are aware of what is happening on an analyst’s topic. The advantages of the community of intelligence are that discussions and documents stay available over time, whereas discussions over email get lost once stopped. Furthermore, all responses in the discussions are visible, whereas in email, you might be excluded and miss a discussion thread. Finally, the alert function of the community of intelligence allows analysts to be noted when new content is added to a certain topic.

Third, it appears that analysts share both content related issues and process related issues. The community of intelligence is used to collaborate on work, as well as talking about the way the work can be done. Interesting to note is that concerning content related issues, in many instances analysts meet each other through the community and start to collaborate outside the community. In discussions you often find phrases like: ‘I can help you, please mail me.’ or ‘We have analyzed that topic last year, please mail or phone me for a copy of the document.’ Apparently the community of intelligence is not considered secure enough within a police context to support sharing content information. As for process related issues, this barrier does not exist. By sharing process related issues, the community of intelligence speeds up the process of developing the analytical work practice. Experiences with new tools, techniques and work practices are shared through the community of intelligence by itself, whereas previously, allocated effort was needed to broadcast information about new tools, techniques and work practices to all analysts involved.

Fourth, the community of intelligence is a non-hierarchical network where analysts are each other’s peers. This is considered of great value for the community to freely share information and questions. Some of the police chiefs and analysts’ supervisors have problems accepting this non-hierarchical framework. They feel the urge to give assignments to the community; not only because they want to be in control, but also because they see the power of the community as a resource that should be guided. Until now, we have been able to keep the hierarchy outside allowing the community to become the secret power of intelligence led policing.

Although the community of intelligence already has shown being the secret behind intelligence led policing, steps for further improvement are recommended.

Sharing content information through the community of intelligence is still a problematic issue. This is due partly to the fact that the police culture is still reluctant to sharing information. And partly, because analysts lack clear guidelines about what to share when and how. A code of conduct for sharing information through the community of intelligence might support analysts in making this judgment. On the other hand, a code of conduct might also feel too restrictive, prohibiting the free flow of ideas and information guided by the needs of the members themselves.

Increasing the network is another thread for development, both in quantity and quality. Already 30% of all potentially interested employees of the Dutch police are member of the community. This leaves room for still an ever stronger growth in quantity. As for quality, currently 90% of the members are employed at a police force, 5% of the members are related to the Police Academy of the Netherlands, and only 5% are affiliated to one of the partners in the security domain, such as customs and the public prosecutor. Increasing the scope of the network might introduce a diversity of information and perspectives that analysts working for the police would not have access to through their normal channels. It is the unexpected information that provided the opportunity to learn and discover.

The implementation of Sharepoint 2007 in the police organization disables a number of functionalities that are considered needed by the analysts and that further enhance the possibilities to really collaborate on issues. A pilot is started in which Sharepoint 2010 enhanced with Newsgator is evaluated for its added value to the community of intelligence. In case of a positive evaluation, this supports the argumentation to invest in new technology to support the community of intelligence.

Finally, the greatest challenge for the community of intelligence is to step up to the next level of collaboration. Currently, analysts share finished products with each other and they ask questions when they start with an analytical assignment. However, what is lacking, is analysts working together through the community of intelligence on an analytical assignment, together producing an intelligence report. A first step towards this goal might be to have peers review your work before it is finalized.

ACKNOWLEDGMENT

The authors would like to thank Mieke Struik, Tobias de Wit, and Daniel Bulten for their enduring enthusiastic efforts in helping to make the community of intelligence work the way it does now. We like to thank Hans Regterschot, Hans Broere, Michel Penterman, Jos Schalkwijk, Gwendolyn Kolfschoten, Eefje Teeuwisse and Gea de Groes for their supporting effort and for translating needs into functional requirements into a technical realization. And we, of course, are grateful to all members of the community of intelligence for using it to share information, knowledge and expertise, and to collaborate through it. Let’s keep up the good work!
REFERENCES