Journal Article

# Secure military social networking and rapid sensemaking in domain specific concept systems: research issues and future solutions

Garside, D., Ponnusamy, A., Chan, S. and Picking, R.

*Future Internet* **2012**, *4*, 253-264; doi:10.3390/fi4010253

OPEN ACCESS

*future internet*

**ISSN 1999-5903**

www.mdpi.com/journal/futureinternet

*Article*

# Secure Military Social Networking and Rapid Sensemaking in Domain Specific Concept Systems: Research Issues and Future Solutions

**Debbie Garside [1,2,*], Arjun Ponnusamy [1,2], Steve Chan [3] and Richard Picking [2]**

[1] GeoLang Ltd., Bridge Innovation Centre, Pembrokeshire SA72 6UN, UK; E-Mail: arjun@geolang.com

[2] Glyndwr University, Mold Road, Wrexham LL11 2AW, UK; E-Mail: r.picking@glyndwr.ac.uk

[3] Massachusetts Institute of Technology GDC, Cambridge, MA 02139, USA; E-Mail: s_chan@mit.edu

* Author to whom correspondence should be addressed; E-Mail: debbiegarside@geolang.com; Tel.: +44-1646-689231.

*Received: 21 December 2011; in revised form: 2 March 2012 / Accepted: 5 March 2012 / Published: 12 March 2012*

---

**Abstract:** This paper identifies the need for a secure military social networking site and the underlying research issues linked to the successful development of such sites. The paper further proposes a solution to the most basic issues by identifying and tackling known potential security threats to military personnel and their families. The paper further defines the base platform for this development to facilitate rapid sensemaking to inform critical communications and rapid decision making processes during abrupt governance and eco-system change, and how the plethora of information (termed as *Big Data*) on social networking sites can be analysed and harnessed. Underlying architectural issues, efficiency and complexity are explored and their future development is considered.

**Keywords:** secure military social network; rapid sensemaking; domain specific concept system; contextualization engines

---

## 1. Introduction

Social networking has been defined as "a web based service that allows individuals to: (1) construct a public or semi-public profile within a bounded system; (2) articulate a list of other users with whom

they share a connection; and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site" [1].

The use of social networking sites (SNS) has burgeoned during the past decade with Facebook, ranked the second most visited web site in the world, now boasting over 840 million profiles who connect to 'friends'. We use the term profile as opposed to user as there is some consternation about the numbers of purported users. Other popular social networking sites include MySpace, Bebo and Twitter. The rapid growth of SNS technologies along with the huge amount of information that has been posted over recent years causes a number of problems associated with *Big Data*, which for the purposes of this paper is defined as unstructured data in excess of one terabyte (http://www.scmagazineuk.com/survey-finds-lack-of-understanding-of-big-data-or-how-to-manage-it/article/229028/?DCMP=EMC-SCUK_Newswire accessed on 24 February 2012). Problems include capture, storage, visualization and analytics (sensemaking), searching, sharing and information security.

As well as public SNS systems, a number of group specific networking sites have also been established with some success. Milsuite, a suite of secure social networking tools, is one such group specific site. Created in October 2009, Milsuite includes MilBook, MilWiki, MilBlog and MilTube (launched October 2010). Designed as a secure Military social network where military personnel, civilians and contractors can share information and knowledge, the suite has been somewhat successful in that it recorded 85,000+ users. An overview of the thinking behind the design of MilSuite can be found at http://markkovacevich.blogspot.com/2010/01/milsuite-military.html. Hosted on the Marine Corps Enterprise Network, MilSuite has been developed by the Communications-Electronics Research and Development Centre of RDECOM but is not intended for use by family and friends of military personnel.

In this paper we concentrate on user habits within publicly available social networking sites, as well as the tools, apps and metadata available and how these may represent significant security issues.

Typical uses of social networking sites (SNS) include: real-time chatting with friends and family, posting of personal information and details of personal events, sharing of interests and personal photographs, posting of biographical details and affiliations including political and religious views, as well as the sharing of contact information–sometimes not their own and without the third party's consent. We will outline how these seemingly innocent user habits may pose significant personal, national and international security threats and detail occasions where operational security has been compromised and classified information posted freely on SNS.

Following the identification and discussion of the potential security threats, we present an architecture that integrates existing popular social networking solutions, that offers significant security threat alleviation, without adversely affecting the privacy, integrity or security of the end user.

## 2. The Need for Secure Military Social Networking

In January 2010, as a result of a request under the Freedom of Information Act, it was reported that in the preceding 18 months the UK Ministry of Defence (MOD) had identified 16 separate occasions where classified information had been leaked via social networking sites. Whilst the majority of MOD administered computer networks do not allow access to social networking sites there are a number of "cyber cafes" established within deployment zones abroad that allow free internet access.

In the US, the Fleet and Family Support Centre of the US Navy gave the following advice to Facebook members related to military personnel:

> *"It is not unprecedented for spouses and family members of U.S. military personnel to be targeted for intelligence collection. This is true in the United States and especially true overseas. Navy family members all know some bits of critical information. It may not be classified, and it may even seem insignificant. But, to the potential adversary, it is a piece of the puzzle. The power of emerging media tools is a two-edged sword: It makes information exceptionally accessible when posted–for anyone who is interested, including potential adversaries."*
>
> (http://www.cnic.navy.mil/CNIC_HQ_Site/WhatWeDo/FleetandFamilyReadiness/FamilyReadiness/FleetAndFamilySupportProgram/CNICD_A065894 accessed on 15 December 2011)

In 2012, India with its third largest active military in the world banned its army from social media of all flavours following threats to national security when four naval officers divulged confidential information on social media. Such measures are now becoming a global scenario with countries like Korea also issuing guidelines to its soldiers on safe use of social media.

Operational Security (OPSEC) and Personal Security (PERSEC) policy documents have been developed and circulated by both the UK Ministry of Defence (MOD) and the US Department of Defense (DOD) in relation to social networking. A number of explanatory documents designed to assist military personnel and their families on OPSEC and PERSEC issues related to social networking have been published during the past few years. Most recently, the UK MOD issued advice on the dangers of a Facebook tool called "Places I checked into". The tool, which has automatically been activated on all Facebook profiles, uses the IP address and a geo-locating system to identify the user's login location which is then displayed on their Facebook profile. The example given of the dangers this poses to military personnel and their families includes the name of the military barracks and a map of the actual location. The document further describes the security concerns:

> *"The main concern relating to the use of the application is that it may inadvertently compromise the locality of a military user. Of significant note, users on operations or in Northern Ireland are potentially putting themselves at risk by drawing attention to their exact whereabouts."*
>
> (http://regmedia.co.uk/2010/10/01/mod_facebook_places.pdf accessed on 15 December 2011)

Poignantly, our paper is written on the very day a young policeman was killed by a car bomb outside his home in Northern Ireland.

The US DOD civilian guidelines define 10 OPSEC points relevant to social networking:

*Don't discuss current or future destinations/ ports of call/deployment base.*
*Don't discuss current or future operations or missions.*
*Don't discuss current or future dates and times of exercises or missions.*
*Don't discuss readiness issues and numbers.*
*Don't discuss specific training equipment.*
*Don't discuss people's names and operations.*
*Don't speculate about current or future operations.*

*Don't spread rumors about current, future, or past operations or movements.*
*Don't assume the enemy is not trying to collect information on you; he/she is.*
*Be smart, use your head, and always think OPSEC when using email, phone, chat rooms and message boards.*

(http://regmedia.co.uk/2010/10/01/mod_facebook_places.pdf accessed on 15 December 2011)

In February 2011, the US Navy issued a 31 page updated slide show defining the recommended Facebook privacy settings for military personnel and their family members. It would be interesting to conduct a survey of military personnel and their family members to establish how many have knowledge of this document and have taken the recommended actions. This document can be found at SlideShare (http://www.slideshare.net/USNavySocialMedia/facebook-privacy-settings-february-2011) and reported just over 16,600 views. Current statistics show that there are nearly 1.5 million personnel employed within the US Military with just over half a million additional civilian personnel employed.

In researching this paper, we reviewed a number of security context related Facebook posts by family and friends of military personnel. Although not conducted as a scientific survey, the result with regard to OPSEC and PERSEC revealed that friends and family of military personnel are deeply concerned about the dangers of social networking with many openly striving to adhere to the OPSEC/PERSEC directives. Many appeared fearful of unwittingly divulging information. Many appeared unsure of their actions. This could be perceived as, perhaps, putting the friends and families of military personnel under a degree of pressure when using social networking sites which may, in some instances, outweigh the considerable gains identified within social networking for those left behind by those deployed on active service.

With ever changing goalposts by way of new apps and the security issues they may pose it is always going to be difficult, if not impossible, to achieve good coverage of new directives for this security conscious social networking group.

Both the UK MOD and the US DOD have offered inconsistent advice on social networking during the course of the past few years; sometimes encouraging and sometimes discouraging their use. Potential good uses of social networking have been explored and utilized within the aforementioned MilSuite secure military social networking tools and also as a facilitatory tool for Family Readiness Officers. As with the UK MOD, the US DOD are working alongside academia to undertake further research and development into secure social networking for families of military personnel.

*"The U.S. Marine Corps, which had once issued an immediate ban of SNS on the Marine Corps Enterprise Network (MCEN) NIPRNET in 2009, is striving to resonate with the spirit of DTM 09-026 and is very desirous of deploying a secure, robust next-generation SSN to better equip their Family Readiness Officers (FRO) for their constituents. The key to achieving this will be to create a new communications system, for families of marines, on a geospatial overlay architecture."*
*MIT GeoSpatial Data Centre, 2011*

Inevitably, given accessibility to a broad range of friends and family, many who may not be within the defined military network, users are frequenting the most popular social networking sites. To try to change these social networking habits will be extremely difficult if not impossible.

Moreover, the value of banning social networking on defence-administered computer networks has diminished to the point of being of no value at all given the prolific take up of smartphones of which

most, if not all, have Facebook and other social networking apps pre-installed. This fact is further emphasised by recent research which predicts the number of mobile social media users to reach 1.3 billion in 2016, surpassing the total number of social media users on all platforms today. (http://www.marketwatch.com/story/mobile-social-media-users-to-reach-650m-in-2011-rising-to-13bn-in-2016-2011-12-19 accessed 24/02/2012). With evermore usage scenarios for smartphones in the field being developed, such as secure GIS location of improvised explosive devices (IEDs), this social networking enabled mobile technology is becoming essential and ubiquitous.

In essence, there are considerable benefits to social networking for military personnel and their families and friends, not least crisis communications via Family Support networks. However, the downside to social networking is the security challenges it creates which at their most severe could potentially compromise OPSEC and/or PERSEC. The personal security of the friends and family of military personnel is also of paramount importance and this can easily be compromised by geo-tagging and additional metadata inadvertently posted on social networking sites within photographs.

Metadata has for some time been a source of security breaches. A well documented security breach within a Microsoft Word document that was posted on the website of the Coalition Provisional Authority (CPA), the American government that ruled Iraq from April 21, 2003, to June 28, 2004, the document metadata contained a previous version with secret security-related information in it.

In social networking, metadata and geo-tagging are causing considerable security concerns. Friedland and Sommer [2] took just 15 min to identify the exact location (±1 m) of a picture of a bicycle in front of a garage door using the stored geo-coordinates. They further articulate:

> *"...it is mostly the high-end smartphones today that have GPS built in, including the iPhone, Android-based devices, and the newer Nokia N-series. An alternative (or additional) method for determining the current location is WIFI access point or cell-tower triangulation: correlating signal strengths with known locations allows a user or service to compute a device's coordinates with high precision... If a device does not directly geo-tag media itself, such information can also be added in post-processing, either by correlating recorded timestamps with a corresponding log from a hand-held GPS receiver; or manually using a map or mapping software."*

There are many similar research papers that document the ease with which a maliciously minded social engineer can trace individuals using metadata gleaned from social networking sites. In addition, there are many open source geo-location tools available, for example Creepy (http://ilektrojohn.github.com/creepy/) and PleaseRobMe.com (http://pleaserobme.com/).

## 3. Discussion and Proposed Solution

The scale and scope of these potential security issues when using social networking sites places the potential user led solutions based on Defence directives either beyond the level of most social networking users or inevitably makes the tasks required to deal with the varying and ever changing solutions too onerous for the average user regardless of their being security minded. A realistic and feasible solution is to build a secure military social networking interface for the major social networking sites that automates the changes required to security settings and performs metadata removal, as well as the numerous tasks (including the masking of IP address and other location based

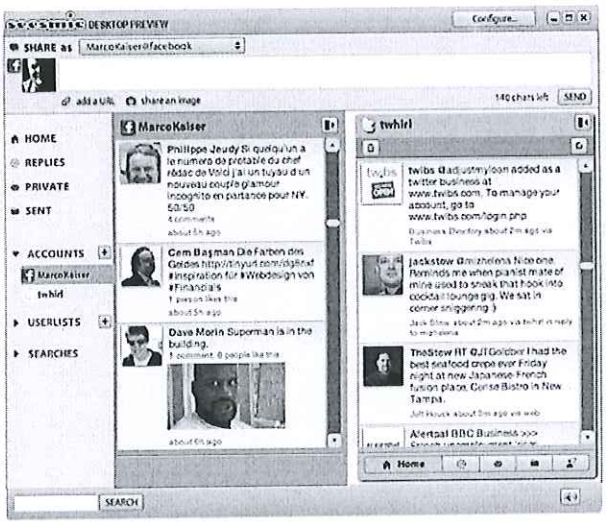
information) required to protect both military personnel and their families. Such a tool would become the recommended app for all military personnel and their families and friends. The tool would be downloaded and installed on home computer systems and mobile devices that can be upgraded and updated as and when new security threats are identified. Defence directives will no longer consist of 31+ pages of "do's", "don'ts" and "how to's" that most likely are never adopted in full by the majority but will rather provide automatic updates to the end user systems taking away the necessity for the end user to implement a designated rules system.

Current US DOD guidelines include advice to social networkers to routinely "Google" their user name to establish current personal information on the web and update profiles accordingly. No information is available as to how many military personnel or members of their families conduct this but it would be relatively simple to incorporate within a secure military social networking interface. It is envisaged that a simple automated reminder system would be incorporated within the interface as proposed later in this paper. Such an interface would ultimately be linked to domain specific rapid sensemaking, with temporal queries associated to the individual user details for conducting automated personal web searches. The term domain specific rapid sensemaking in this context denotes specific contextualized intuitive information.

The US DOD already provides antivirus software for personal use. To what level this service is taken up by military personnel and their families remain unknown. However, a secure social networking interface could incorporate this service, creating a security solution that integrates important aspects of human and machine security.

Our solution is named SNeSSI, an acronym for "Social Networking Site Security Interface". The implementation of SNeSSI makes use of the open source features of the most popular SNS, such as Facebook and Twitter. The API (application program interfaces) for these offer software developers the ability to feed communication between the user and the site through a filter (the SNeSSI), that can monitor and intercept data streams, and advise a user should their actions raise cause for concern. A very simple example of such an interface, called the Seesmic Desktop, has been developed to demonstrate the functionality of Facebook's recently released Open Stream API, as shown in Figure 1.

**Figure 1.** Seesmic Desktop (http://blog.seesmic.com/2009/04/facebook.html).



This system combines Facebook and Twitter feeds into one integrated application. Whilst we are not proposing a security-rich clone of this system, the example clearly demonstrates the feasibility of the SNeSSI concept, and this approach can easily be migrated to other platforms, including smartphones and the other mobile devices that form the "Internet of Things".

Another example that uses a similar architecture is Apache Wave in a Box (WiaB), previously known as Google Wave (http://www.waveprotocol.org/). Although this is not a SNS, the concept of feeding information from a other native applications into one integrated client interface is the same. However, this system is different in that all communications are stored on a central server, which would be more robust and controllable from a security point of view, but would be more difficult to integrate the existing SNS user experience. This raises an important issue, in that usability must not be compromised by the adoption of a SNeSSI, otherwise some users will ultimately choose to by-pass it, no matter what the consequences might be. One of the main reasons that Google abandoned its Wave project was that not enough users were taking it up, many citing its poor usability as a fundamental issue, including problems with its stability, flexibility and security. The user interfaces for Seesmic Desktop and WiaB are very similar, and lessons have been learned not to make the same usability mistakes for the SNeSSI.

It is not uncommon to view security and usability as two inversely proportional entities within cyber security. DeWitt and Kujis endorse this fact with their work titled, "Is usable security an oxymoron?" [3]. Various other works [4–6] identify the major usability problems that arise as a result of the aforementioned conflict. Unmotivated users, abstract security policies, lack of feedback, fractured security options and increasing complexity of software systems are the key problems affecting usability. Achieving the competing goals of security and usability is regarded crucial to the success of the system. Research into cyber security usability evaluation methods unveiled two major approaches namely user studies and expert-based evaluations [7,8]. Techniques such as laboratory-based user testing, user observations, questionnaires and semi-structured interviews are employed in user studies while expert-based evaluation involves usability experts judging the usability of the system through cognitive walkthroughs and heuristic evaluations [8,9]. Appropriate guidelines for usable security which include early consideration of security, giving guidance and recommendations to users are enlisted by Jason *et al.* [10]. By employing the above techniques and guidelines, the proposed user interface design will be developed in consultation with the targeted users, including military personnel, their families and friends. We are also in the process of conducting preliminary usability evaluation of the SNeSSI concept with small focus groups using techniques outlined by Rubin *et al.* [11] and following human-centred design approaches detailed in ISO 9241-210 [12].

Current simple interfaces have demonstrated proof of concept and essential utility of the system, and more novel futuristic interfaces are being investigated. One such area under investigation is to use avatar technologies to form a dialogue with a user, should there be a requirement to intervene in their activity. The intelligence behind the avatar interface would report back to a central resource in potentially serious security breach scenarios. This intelligent aspect of the SNeSSI is based on Contextualization Engine and Rapid Sensemaking (CERS) technologies. With an underlying knowledge base, the SNeSSI avatar could intervene when keywords or phrases, such as barracks, location data, mission names etc., were posted, prior to the post being made live on the social

networking site offering intelligent intervention. The CERS aspect of the SNeSSI interface plays a dual role in that it is able to access military personnels' online "friends", analysing their details and posts, which may identify "malicious information groomers" or social engineers who also pose a security risk. This aspect of the interface could result in dynamically created domain specific concept systems combined with temporal geospatial ontology to be used in conjunction with a future military devised ontology and its underlying concept system and knowledge base which would facilitate contextualisation. The ability to save analysis and insights on a given scenario with the ability to also run the same analysis according to temporal and/or geospatial data would result in meaningful data analysis over time and place. However, this may result in large repositories of data.

CERS may also integrate effectively with the current US military initiative Operation Earnest Voice (OEV) where US military personnel are operating as many as 10 avatars/profiles collecting information on possible terrorists. Whilst reportedly only being utilised in foreign languages (Arabic, Pashto, Urdu and Farsi), OEV could be expanded to identify would-be malicious social engineers with the information fed into the SNeSSI. This information about potential terrorists may highlight malicious information groomers and social engineers found within the 'friends' of military personnel and/or their family's profiles, thus forming a degree of protection. It could also be utilised for feeding misinformation back to these malicious social engineers.

In the context of rapid sensemaking within military family support, the interface can offer advice or guidance by way of interface advertisements e.g., financial assistance, social relationship counselling, family assistance and many other military personnel targeted services which may be proffered to users of SNeSSI at relevant times e.g., if the words 'feeling' 'down' 'depressed' or 'sad' are posted the member can receive an advertisement for Family Support Services. In this context, the interface may also assist in identifying worrying trends either at home or abroad. The key is in the design of a contextualization engine that supports such rapid sensemaking and ultimately also supports decision-making from the overall analysis of themes identified. Adhoc qualitative research in military forums undertaken as part of the background research has shown that such automated interventions, in particular in relation to the "do's" and "don'ts" of secure military social networking, would lead to a sense of secureness.

In addition to CERS, visual analytics linked to IP address could display the general mood of groups of friends and family which could, perhaps, be linked to military intelligence e.g., even a small amount of knowledge of critical missions may affect the mood of friends and family. News reports may also have an effect, for example reports of lack of equipment. It is important for the military to make sure that the families of personnel on active duty overseas are taken care of, as worries from home can affect performance in the field. A method for offering reassurance and support, by way of targeted military advertising as a direct result of contextualization and rapid sensemaking, in an unobtrusive way and without the end user realising they have been targeted, would be highly valuable.

The use of data mining and Automated Reasoning (AR) will inform a human analyst defined ontology and assist the sensemaking and ranking process. Visual analytics and query expansion techniques will inform this rapid sensemaking process.

Queries can be saved and scheduled for temporal re-run with results highlighted when significant changes take place. As well as user defined ontology, temporal data mining of terms within social networking environment can enhance an analyst's ability to detect new themes for inclusion in the

ontology—perhaps linked to place and time. This could be used to detect and protect military related "friends". However, it could also be used to trawl social networking posts in general.

Tomaszewski *et al.* [13,14], in their SensePlace application, defined the following components to their sensemaking application: a lexicon, grammar defining multimodal language used by the system for input and output, a discourse analysis model, a user model and a knowledge base of task domain and interface information. The knowledge base may contain information about concepts such as military bases, missions, weapons as well as HCI concepts such as verbal expressions for domain concepts. In the context of rapid sensemaking within a social networking environment, a lexicon of "textspeak" linked to a thesaurus would prove most useful as would algorithms for modifying the ratings of entities within a discourse model. An integrated module could provide information and movement on profiles via geo-tagged data.

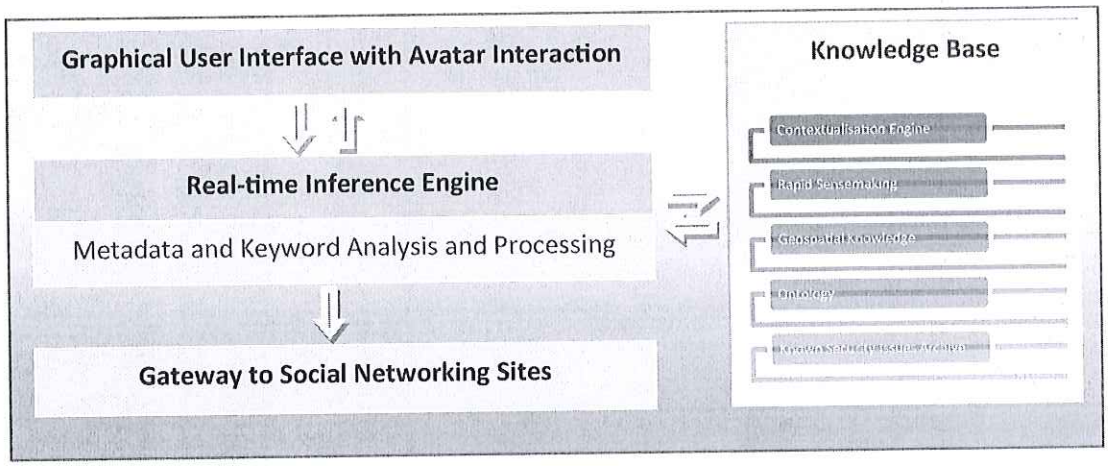
Dynamic global supply chains and the increased geographic responsibilities of decision support systems (DSS) have underscored the need to quickly analyze large datasets so as to adequately engage in the realm of rapid sensemaking (querying, analyzing, etcetera) for security-related processing. While many enterprise systems were previously principally architected and optimized for performance, next-generation intelligent engineering system approaches necessitate architecting and engineering, robust security focussed systems to be evolutionarily resilient and defensible in real time. There is currently a paradigm shift in dataset/computation amalgams — the utilization of the quicker computational intelligence technique of moving the computation to the data instead of the traditional methodology of moving the data to computation is driving a need for real-time High Performance Computing. The processing speed advantage of such systems, on the order of several magnitudes, immediately alters the outcomes of numerous cyber security cost-benefit analysis (CBA) models; the prior return on investment (ROI) considerations and management inclinations that certain cyber security technologies are preliminarily obviated because they may hinder productivity are now being reversed. Thus an entire spectrum of cyber defence approaches predicated upon this newly validated corpus of viable defence-in-depth contributions come into play creating new opportunities for real-time architectures supporting real-time services such as the contextualisation and rapid sense-making as defined within SNeSSI.

In many of these core analytics cases, real-world applications require algorithms that can return within minutes rather than hours; intrinsically, they rely upon the aforementioned sensemaking to locate the pertinent relevance over very large data volumes in quasi-real-time. Furthermore, with every new observation from the myriad of artificial/human sensors, these sensemaking algorithms, which take advantage of this operational tempo, can very readily be configured for the conjoining of diverse data within the same data space and discriminating relationships for expressive context accumulation (ECA), whilst distinguishing noise (e.g., re-tweets) for robust semantic reconciliation (RSR). In the context of SNeSSI this means real-time metadata and keyword analysis and processing with real-time feedback via an avatar as depicted in Figure 2.

The Graphical User Interface with its intuitive design and an animated avatar ensures users' interest in SNeSSI. A real-time inference engine, the linchpin of the architecture, controls the GUI and is informed by an extensive knowledge base comprising of CERS engine, geospatial knowledge, ontology and an archive of known security issues. The inference engine is responsible for making an informed decision about the risk factor associated with the user's interaction with SNS and enriches

the knowledge base. The inference engine also feeds into the Gateway component which acts as the communication bridge between SNeSSI and various commercial SNS.

**Figure 2.** SNeSSI Overview.




## 4. Conclusions

This paper focussed on a number of issues relating to social networking within the military. Issues identified included security in relation to military information, military personnel and their families and friends. The age old problem of information leakage, previously associated with word of mouth, has migrated to the web and, in particular, social networking with its ability to easily share information and inadvertently give information away via associated metadata. In the past, various solutions have been proffered for this well documented problem. However, the SNeSSI concept deals with the identified problems in a holistic way whilst adding a new dimension in the form of intervention and interaction through the inference engine and avatar. The proposed concept could also be adopted by commercial organisations looking to protect sensitive data. There is also a need to develop systems and architectures that can cope with today's Big Data and its real-time analysis that will ultimately support the concept.

Big Data and linked data have recently become the buzz words of the World Wide Web and necessarily so. Pulling all this data together into a valuable resource that can be used to inform and protect is the emphasis of many projects. The plethora of unstructured data available within cyber space today necessitates the building of new and innovative systems that can analyse and classify this currently unstructured data with the aim of forming useful information and conceptualized knowledge bases. Harnessing the Big Data that is representative of social networking today is not a trivial task. We believe that this paper outlines the importance of harnessing and utilizing Big Data from social networking whilst offering an automated intervention through rapid sensemaking that will support secure military social networking.

## 5. Future Works

Finding the delicate balance between preserving user experience with SNS while ensuring security to the stakeholders involved would lead to a comprehensive architecture incorporating several facets of

SNeSSI. The possibility of SNeSSI to orchestrate other security solutions to ensure privacy will also be investigated. Web browsers have evolved over the years from a simple client program to a sophisticated interactive platform influencing most aspects of Internet usage. Arguably the most preferred communication portal of networked computers, the need for ensuring secured access to SNS through browsers by military personnel and their family cannot be ignored. The fact that browsers have high level access to sensitive personal information despite the usage of cryptographic techniques such as encryption necessitates widening the scope of SNeSSI to include browser environments. Most of today's modern browsers allow significant functional enhancements through extensions. Browser extensions through careful coordination and management of browser events could significantly improve the user experience without having any impact on the actual content. A browser extension working in parallel with SNeSSI to restrict or suggest safe SNS interaction strategies for military personnel and families would bring a holistic solution to the problems identified earlier.

Although this paper has focussed on the security of military personnel and their families, there is much scope for the development of managed social networking within both home and workplace.

## References

1. Boyd, D.; Ellison, N. Social network sites: Definition, history and scholarship. *J. Comput.-Med. Commun.* **2007**, *13*, 210–230.
2. Friedland, G.; Sommer, R. Cybercasing the Joint: On the Privacy Implications of Geo-Tagging. In *Proceedings of the Fifth USENIX Workshop on Hot Topics in Security (HotSec 10)*, Washington, DC, USA, 11–13 August, 2010.
3. DeWitt, A.J.; Kuljis, J. Is usable security an oxymoron? *Interactions* **2006**, *13*, 41–44.
4 Whitten, A.; Tygar, J.D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, Washington, DC, USA, 23–26 August 1999; pp. 169–184.
5. Sasse, M.A. Usability and trust in information systems. Available online: http://www.dti.gov.uk/files/file15320.pdf (accessed on 7 March 2012).
6. Furnell, S. Why users cannot use security. *Comput. Secur.* **2005**, *24*, 274–279.
7. Chiasson, S.; van Oorschot, P.C.; Biddle, R. A Usability Study and Critique of Two Password Managers. In *Proceedings of the 15th USENIX Security Symposium*, Vancouver, BC, Canada, 31 July–4 August 2006; pp. 1–16.
8. Bennett, D.J.; Stephens, P. A cognitive walkthrough of autopsy forensic browser. *Inf. Manag. Comput. Secur.* **2009**, *17*, 20–29.
9. Rosenbaum, S. Usability evaluations versus usability testing: When and why? *IEEE Trans. Prof. Commun.* **1989**, *32*, 210–216.
10. Nurse, J.R.C.; Creese, S.; Goldsmith, M.; Lamberts, K. Guidelines for usable cybersecurity: Past and present. In *Proceedings of the 2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, Milan, Italy, 8 September 2011; pp. 21–26
11. Rubin, J.Z.; Chisnell, D.; Spool, J.M. *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective tests*, 2nd ed.; Wiley Publishing: Indianapolis, IN, USA, 2008.

12. *Ergonomics of Human-System Interaction—Part 210: Human-Centred Design for Interactive Systems*; International Organization for Standardization: Geneva, Switzerland, 2010; ISO 9241-210.
13. Tomaszewski, B.; Blanford, J.; Ross, K.; Pezanowski, S.; MacEachren, A. Supporting rapid sense making in diverse web document foraging computers, environment and urban systems. *Comput. Environ. Urban Syst.* **2011**, *35*, 192–207.
14. Tomaszewski, B.; MacEachren, A. Geo-Historical Context Support for Information Foraging and Sensemaking: Conceptual Model, Implementation, and Assessment. In *Proceedings of 2010 IEEE Symposium on Visual Analytics Science and Technology (VAST)*, Salt Lake City, UT, USA, 25–26 October 2010; pp. 139–146.