Managing the Risks of Social Media in the SAF

by **CPT Lee Hsiang Wei**

Abstract:

Social media is a type of online media that expedites conversation through the creation and exchange of user generated content targeted at peers. This unprecedented level of interaction makes social media appealing and attractive to many around the world. With the speed at which social media grows and multiplies, the Singapore Armed Forces (SAF) cannot afford to ignore risks already exploited both within and outside of the military context. SAF's social media policy needs to continually adapt quickly as new trends in social media emerge. By ensuring several key thrusts are achieved, social media will become a manageable medium without compromising information and operational security in the Armed Forces.

Keywords: Security; Communication Technologies; Military Policy; Adaptability and Flexibility

INTRODUCTION

What is Social Media?

Social media represents a shift in the way we as a culture communicate. Social media is a type of online media that expedites conversation through the creation and exchange of user generated content targeted at peers. Examples of social media include Facebook, Twitter, Flickr and YouTube (see Figure 1). The key feature of social media is that it provides the common user with highly accessible and scalable publishing technologies.

Social media provides new ways to connect, interact and communicate. Users can post comments and photos, update their online profiles and even reflect their mood to others. These "sharings," once posted, are instantly available to the other users of social media, increasing the rate of which users interact with one another. This unprecedented level of interaction makes social media appealing and attractive to many around the world.

Social Media and the SAF

The appealing and attractive nature of social media has made it a mainstay in the way we live, work and play. The social media industry has been experiencing phenomenal growth locally and worldwide over the past couple of years.[1] With the rise in popularity of mobile computing with devices like tablets and smartphones, users are able to update their online presence wherever and whenever, as well as keep abreast of the updates posted by their friends and family.

Figure 1: Examples of Social Media

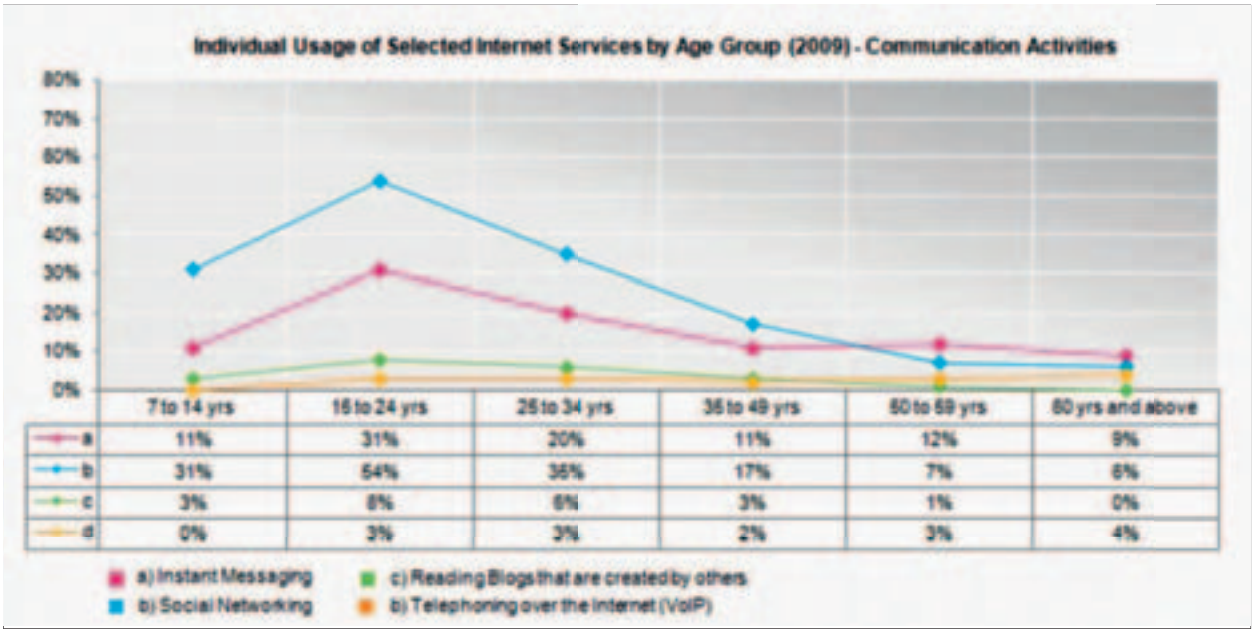


Figure 2: Individual Usage of Selected Internet Services by Age Group in 2009[2]

The use of social media in Singapore includes all age groups, with youths from 15 to 34 years accounting for the majority of social media users (see Figure 2). Some of the more popular forms of social media in Singapore include Facebook and Twitter, which have a significant following of approximately 2.5 million and 2.1 million users respectively.[3]

Although there are no official statistics documenting the use of social media in the Singapore Armed Forces (SAF), it is safe to assume that the service members in the SAF will probably exhibit the same usage patterns as the average Singaporean. Our service members may not use camera phones due to our security policies, but the smartphones that most carry still grant them access to social media even while at work. Surveys have shown that compared to the average web user, mobile users utilize social media more extensively (see Figure 3). While social media allows our service members to feel a greater connection to family and friends, it brings about risks as well as potential security implications for the SAF. This means that the SAF cannot afford to ignore the use of social media by its service members.

Figure 3: Mobile users utilize social media more extensively than the average web user[4]

This essay sets out to highlight some of the more prominent risks brought about by the use of social media faced by the SAF and provides some recommendations to mitigate these risks while embracing the social media phenomenon.

Risks Associated with Social Media

There are five key risks that the SAF faces while embracing the social media phenomenon—Risk Through Direct Disclosure, Risk Through Revealing Locations, Risk Through User Anonymity, Risk by Design and Risk from Information Aggregation. These risks can be categorized into two broad types—user-

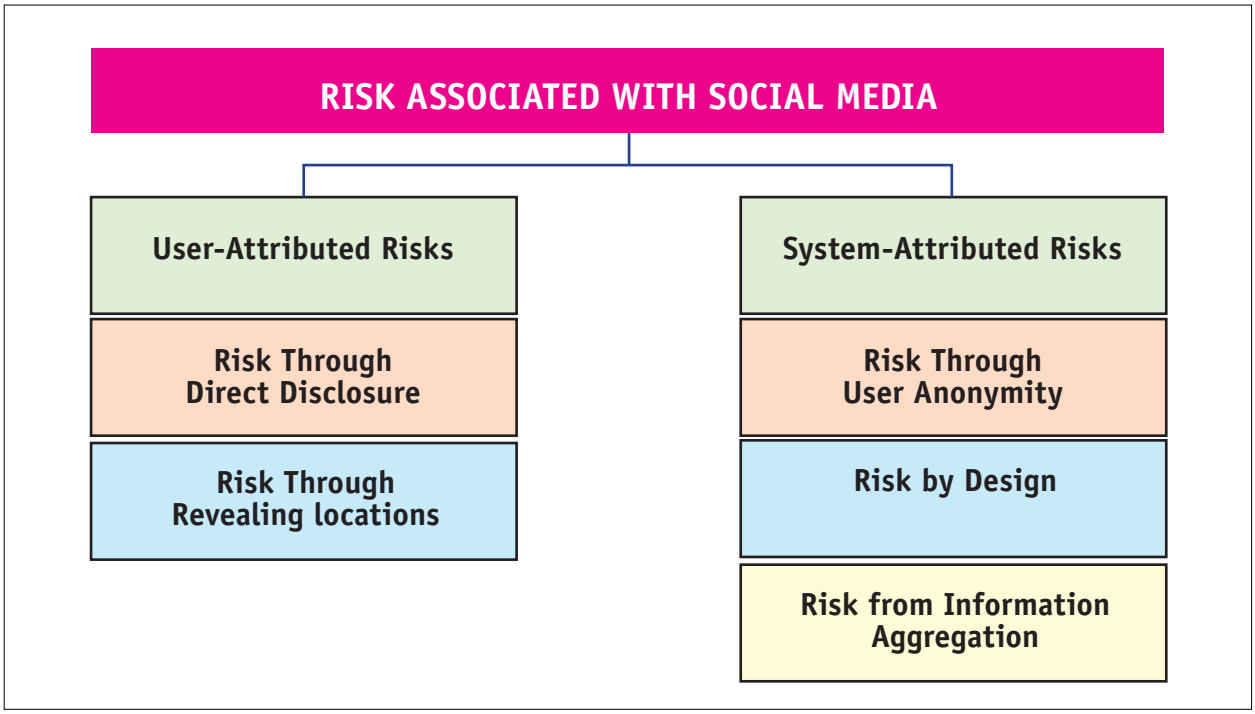


Figure 4: Risks Associated with Social Media

attributed risk and system-attributed risk. In the SAF context, user-attributed risk is where the risk originates from the actions of the service member while system-attributed risk is where the risk originates from the inherent characteristics of social media platforms. The following diagram summarizes these risks (see Figure 4).

1) Risk Through Direct Disclosure. Given the nature of social media, which hinges on the creation and exchange of user generated content, users are encouraged to share information about themselves. SAF service members may at times not think twice about sharing their private thoughts in their social media accounts, inadvertently revealing sensitive information to other users on social media. This direct disclosure of sensitive information posted compromises Operational Security (OPSEC).

Some of the sensitive information that may be posted online can include classified information about military organization, tactics and capabilities. These violations of OPSEC can possibly go as far as to affect national security and compromise safety of ongoing operations. In March 2010, the Israeli military was forced to abandon plans to conduct a raid on militants in a Palestinian village after a soldier posted the location and time of the planned raid on his Facebook page.[5] The consequences would have been catastrophic if the raid was not called off and the militants knew of the impending arrival of the Israeli military.[6]

2) Risk Through Revealing Locations. Another risk is revealing locations of sensitive military installations or military assets in ongoing operations. This primarily manifests itself through the sharing of photos on social media as well as use of location-based services.

When a photograph is taken and uploaded to social media, it can contain information on the location of the image.[7] Many cameras and cell phones sold today are capable of "geotagging," embedding geographical data into the photos.[8] This geographical data can be extracted from the photos even after uploading to the social media platforms. Hence, even though the photographed image does not contain any sensitive information, the embedded geographical data may compromise OPSEC.

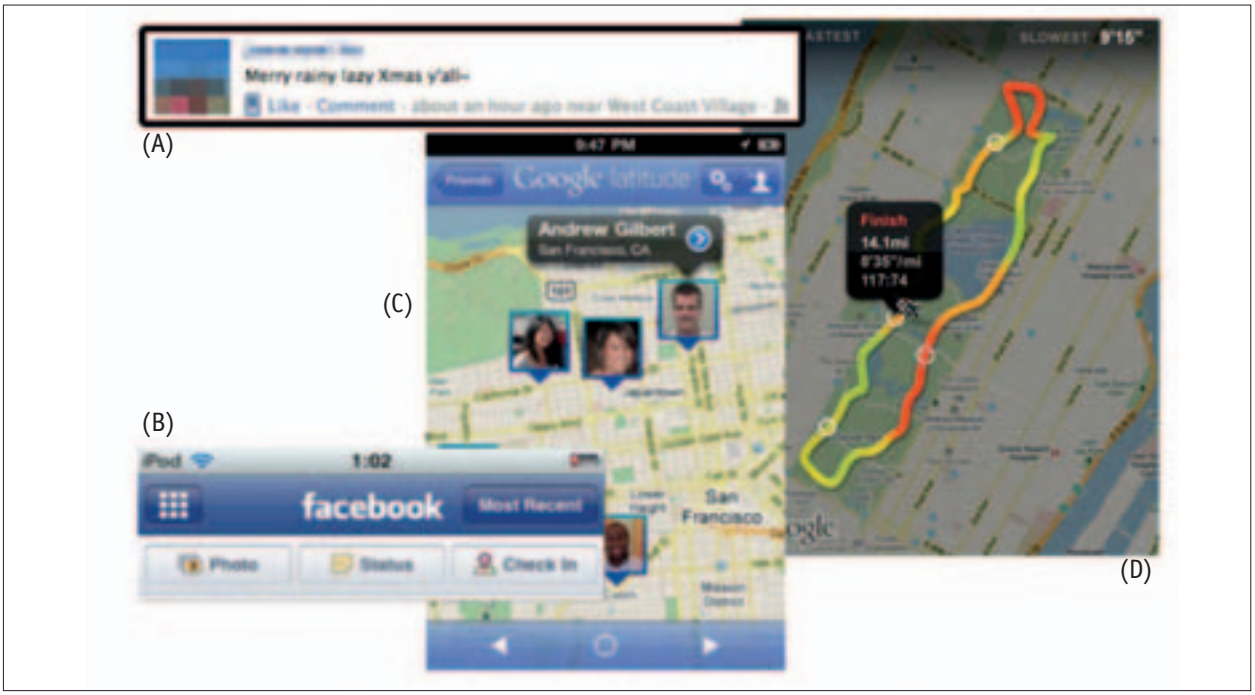


Figure 5: Various Location-Based Services on Social Media (A) Facebook Profile Status, (B) Facebook Check-In, (C) Google Latitude and (D) Nike+ Running App

There are also a variety of location-based services available on social media today, including Facebook profile statuses, Facebook check-ins, Google Latitude and applications that track users' movement, i.e. Nike+ Running App (see Figure 5). These location-based services are targeted at the users of mobile devices, encouraging them to update (knowingly or unknowingly) their geographical locations online. In December 2010, the US Army banned the use of "location-aware" applications on government-issued smartphones due to intelligence that the sudden increase in US soldiers being targeted by enemy snipers was a result of their adversaries making use of locations published on social media.[9]

3) Risk Through User Anonymity. The current state of social media lacks the necessary processes to verify the authenticity of users. There are users who take advantage of this "loophole" to create and maintain anonymous and fictitious user profiles. It is possible for a user with malicious intent to use a false identity to establish links and gain access to otherwise private information.

The "Robin Sage" experiment discussed in the BlackHat security conference in January 2011 highlighted the ease of obtaining classified information via a fictitious profile. The Robin Sage Experiment entailed creating a blatantly false identity of a female claiming to work in the military intelligence industry.[10] It involved convincing but fake social media under the alias "Robin Sage" which included a photo of a cute girl borrowed from an adult website (see Figure 6), and the job title of "Cyber Threat Analyst."[11] At the end of the experiment, "Robin" accumulated hundreds of connections through various social networking sites.[12] Throughout the duration of the experiment "Robin" was offered gifts, government and corporate jobs, and options to speak at a variety of security conferences.[13] More alarmingly, some of the information revealed was classified in nature and which "Robin" should not have been privy to.[14] It was discovered after the experiment that an inspection of the "Robin Sage" profile would have uncovered its fictitious nature. The outcome of this experiment is particularly embarrassing, given the numerous warnings security professionals preach about the dangers of the social media. Although this

Figure 6: Photo of "Robin Sage"

"Robin Sage" incident was purely an experiment, there have already been several instances where enemy organizations have used the anonymity of social media to obtain intelligence.[15]

4) Risk By Design. As social media sites function on the basis of exchanging and sharing user generated content, the default settings of most social media platforms tend to maximize visibility of personal information and the minimize privacy. In fact, most privacy measures currently in place in social media platforms are a result of user demands and requests.

Taking Facebook as an example, its approach to privacy was initially network-centric, where the users content was only visible to all other students in the same campus. This gradually changed where Facebook allowed users to determine which information could be shared with whom, with options of "No-one," "Friends" or "Friends of Friends." Subsequently, Facebook allowed companies to create applications for its users and user content could be shared with these third party developers. Over time, Facebook added the ability for users to share their information with "Everyone." Whenever Facebook introduced new options governing content sharing, the default was for the user to share as broadly as possible.[16]

One of the more prominent instances of this happened in December 2009 when Facebook required its users to reconsider their privacy settings. These contents included "Posts I Create," "Status," "Likes," "Photos" and "Notes." For each item, the two choices available where "Everyone" or "Old Settings," with the toggle buttons defaulted to "Everyone."[17] As this prompt was mandatory, users had to select an option before they were able to continue using the rest of the site. Faced with this obligatory and troublesome prompt, many users would have unthinkingly accepted the defaults, allowing much of their content to be more accessible that previous.

5) Risk from Information Aggregation. The risk of information aggregation stems from the potential for an alert adversary gathering and harvesting social media data of our service members, collating various bits of personal information such as family members, friends, social circles, addresses as well as contact information.

Data mining on social media is easy. In February 2010, Pete Warden, an academic researcher wrote a script that managed to harvest 215 million public profile pages from Facebook before being discovered.[18] Pete Warden commented that "... the data ... is still crawlable by anyone else and there are a lot of commercial companies that have grabbed the same dataset."[19] Data mining on social media is perhaps more prevalent than commonly perceived. A more malicious attempt to target military personnel would definitely be more subtle and it would probably go undetected. There are already reports and known instances of such information gathering on social media.[20]

The alert adversary will, over a period of gathering such data, be able to make sense of them and arrive at a more complete set of information. This set of aggregated information can reveal classified information about the military organization, its tactics and even capabilities.

CURRENT STATE OF AFFAIRS

SAF Social Media Policy

The current SAF policies do not address the use of social media well. These policies are largely an extension of the policies pertaining to traditional media. Hence, the policies lag behind the rapid developments occurring in the social media space. The result is that the understanding of the appropriate use of social media varies considerably across the service members in the SAF. A quick survey of our service members' accounts on Facebook shows varying degrees of personal and work-related information displayed on their profiles. These information include their employer, vocation, unit as well as their location of their unit, deployment or detachment.

Other Approaches to Social Media

The US military's approach to social media was a haphazard and fragmented affair where the various services had different and sometimes conflicting policies on social media (see Figure 7).

It was only recently that the US Department of Defense (DoD) standardized their policies across their various services and published guidelines for service members who use social media in a personal capacity.[21] These guidelines attempt to educate their service members on what is inappropriate to post online. The US Central Command has published best practices, lists of "dos and don'ts" as well as articles on how to protect oneself on social media sites. In addition, the US Army recently published a *Social Media Handbook* (see Figure 8) in January 2011 that attempts to delineate the US Army policy on social media.[22]

Figure 7: Haphazard State of Guidelines on Social Media within the US Military (Megan)

There is not much literature regarding the social media policy of other militaries. However, it has been reported that the Chinese Military High Command has also published a list of "70 Forbiddens" which include staying away from social media websites such as Facebook.[23] The Israeli Army, on the other hand, has banned social media after multiple soldiers shared sensitive or embarrassing data via Facebook and other social media.[24]

RECOMMENDATIONS

As we attempt to refine our social media policy, we should keep in mind an underlying principle—when SAF service members participate in social media on which they may be identified or associated with the SAF, they must be cognizant of their appearance as they are representing the SAF and Singapore. There are risks involved when service members use social media, but it may not warrant the need to ban its use, like what the Israeli Army has done. Instead, this essay proposes a three-pronged approach—Education, Clear Boundaries & Guidelines and Support Processes—that will allow service members to continue using social media in their personal capacity without posing undue risks to the SAF.

Figure 8: US Army Social Media Handbook

Education

The first thrust to mitigate the risks of social media is to embark on a rigorous education campaign. This should consist of lessons incorporated into the various initial training schools such as Basic Military Training (BMT), Specialist Cadet School (SCS) and Officer Cadet School (OCS), sessions to update the service members on the new developments and changes in the operational units as well as subsequent courses. When crafting the SAF's social media curriculum, it is important that it goes further than platitudes like "Be Aware" and "Be Careful." The curriculum should leave no doubt in the service member's mind regarding playing his or her part. The education process should have an emphasis on communicating and convincing service members of the risks associated with social media. Relevant real life examples should also be incorporated into these lessons to give service members a better appreciation and awareness of the risks involved in using social media. The education process should be a regular one given the constant influx of new service members into the SAF as well as the ever-changing social media landscape. The curriculum should be regularly reviewed and updated with new developments in the social media landscape. Given the pace of change in social media, it is not surprising that frequent updates will be required to ensure that the syllabus continues to remain relevant.

When SAF service members participate in social media on which they may be identified or associated with the SAF, they must be cognizant of their appearance as they are representing the SAF and Singapore.

Clear Boundaries & Guidelines

The second thrust is for the SAF to establish clear boundaries and guidelines for service members to follow. In this aspect, we ought to learn from the US Army by having a publication similar to the *US Army Social Media Handbook*. The 39-page handbook lays out guidelines as to how the US Army should handle social media and it includes useful checklists as well as procedures for both commanders and soldiers. The handbook also highlights "danger areas" that can cause a service member to innocently reveal more than he should. By having a handbook or a guide easily available, every service member has literature to fall back on whenever in doubt about the use of social media. The handbook should lay out guiding principles that service members should always follow when using social media. In addition, it would be useful to include simple examples of what to do and what not to do, as well as a "Frequently Asked Questions" (FAQ) section to answer common issues. This would go a long way towards providing greater clarity on the SAF's expectations of service members when using of social media. Additionally, there also should be a "one-stop" centre to answer queries and clarifications

that service members may have regarding SAF social media policy. Answers to these queries should also be accumulated and shared with other service members, via circulating updates, including them in the curriculum or updating the FAQ in the handbook. The ideal end state is one where social media culture within the SAF would self-police to actively minimize the associated risks of social media.

Support Processes and Structures

The third thrust is for the SAF to set up supporting processes and structures to keep up with the ever-changing social media space. The SAF has to be able to keep up with the added functionalities that gain rapid following in social media. A dedicated team should be set up to maintain a direct oversight of the social media issues faced by the SAF. This team should not only comprise those senior enough to make executive decisions, but also a representative sample across the various age groups so as to better understand their perspectives on using social media. For example, the younger service members can bring to the table their knowledge of the latest trends and developments in social media, so that changes to curriculums or updates to policies can be made in a timelier manner.

The SAF's social media policy needs to continually adapt quickly as new trends in social media emerge. Educating our service members on the risks associated with social media, establishing clear boundaries and guidelines as well as the timeliness of reviewing the social media policy needs to be a constant endeavor with a high priority.

This team should also be responsible to develop and maintain the social media curriculum, manage the "one-stop" centre for SAF service members, keep abreast of social media developments and to take ownership over SAF social media policy.

CONCLUSION

Social media increasingly plays an important role in personal communication and entertainment. Given the speed at which social media grows and multiplies, the SAF cannot afford to ignore the risks brought about by social media. These risks are very real and this essay has demonstrated that these risks have already been exploited both within and outside the military context.

SAF social media policy needs to continually adapt quickly as new trends in social media emerge. Educating our service members on the risks associated with social media, establishing clear boundaries and guidelines as well as the timeliness of reviewing the social media policy needs to be a constant endeavor with a high priority. By ensuring these three key thrusts are achieved, social media will become a manageable medium with which service members are able to communicate the right messages without compromising information and operational security in the Armed Forces.

The SAF needs a proactive social media policy. If trained and seasoned security professionals can be guilty of letting down their guard, as shown in the Robin Sage Experiment, our service members would require even more knowledge and ongoing training to safeguard the SAF against the risks of social media.

BIBLIOGRAPHY

Bloch, Ethan. "How are Mobile Phones Changing Social Media?" *FlowTown*. 30 March 2010. http://www.flowtown.com/blog/how-are-mobile-phones-changing-social-media?display=wide.

Bonneau, Joseph, Jonathan Anderson, and George Danezis. "Prying Data out of a Social Network." 21 September 2011.

Bowes, Ron. "Return of the Facebook Snatchers." *Skull Security*. 26 July 2010. http://www.skullsecurity.org/blog/2010/return-of-the-facebook-snatchers.

Boyd, Danah and Eszter Hargittai. "Facebook Privacy Settings: Who Cares?" *First Monday* 15, no. 8 (2010).

Constantin, Lucian. "Israeli Army to Block Social Networking over Security Concerns." *Softpedia*. 22 October 2010. http://news.softpedia.com/news/Israelian-Army-Blocks-Social-Networking-over-Security-Concerns-162515.shtml.

Dunnigman, James. "Things Chinese Soldiers Are Not Allowed To Do." *Strategy Page*. 21 June 2011. http://www.strategypage.com/dls/articles/Things-Chinese-Soldiers-Are-Not-Allowed-To-Do-6-21-2011.asp.

Ewing, Phil. "The Terror Threat at Sea." *Military Times*, 31 December 2009. http://militarytimes.com/blogs/scoopdeck/2009/12/31/the-terror-threat-at-sea.

Fabrizio, Elliott. "Dangers of Friending Strangers: the Robin Sage Experiment." *Armed with Science*. 21 July 2010. http://science.dodlive.mil/2010/07/21/the-dangers-of-friending-strangers-the-robin-sage-experiment/.

"Facebook Statistics by Country." *SocialBakers*. 13 September 2011. http://www.socialbakers.com/facebook-statistics/?interval=last-week&orderBy=penetration# chart-intervals.

Flatley, Joesph L. "US Army Connecting Soldiers to Digital Applications Program Putting Smartphones in Soldiers' Hands This February." *Engadget*. 14 December 2010. http://www.engadget.com/2010/12/14/us-army-connecting-soldiers-to-digital-applications-programs-put.

Giles, Jim. "Data Sifted from Facebook Wiped After Legal Threats." *New Scientist*. 31 March 2010. http://www.newscientist.com/article/dn18721-data-sifted-from-facebook-wiped-after-legal-threats.html.

Goodchild, Joan. "The Robin Sage Experiment: Fake Profile Fooled Military Intelligence, IT Security Pros." *Veterans Today*. 11 July 2010. http://www.veteranstoday.com/2010/07/11/the-robin-sage-experiment-fake-profile-fooled-military-intelligence-it-security-pros.

"IDA Singapore: Infocomm Usage – Households and Individuals." Infocomm Development Authority. 14 September 2011. http://www.ida.gov.sg/Publications/20070822125451.aspx.

Katz, Yaakov. "Facebook Details Cancel IDF Raid." *Jerusalem Post*. 3 April 2010. http://www.jpost.com/Israel/Article.aspx?id=170156.

Leyden, J. "Israel using Facebook as 'Spying Tool' in Gaza." *The Register*. 7 April 2010. http://www.theregister.co.uk/2010/04/07/facebook_spying_gaza.

McCloskey, Megan. "When It Comes To Social Media, Military is Anything But Uniform." *Stars and Stripes*. 6 August 2009. http://www.stripes.com/news/when-it-comes-to-social-media-military-is-anything-but-uniform-1.93810.

Murphy, Kate. "Web Photos That Reveal Secrets, Like Where You Live." *New York Times*, 12 August 2010. http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html.

"US Army Social Media Handbook is Here!" 20 January 2011. http://armylive.dodlive.mil/index.php/2011/01/u-s-army-social-media-handbook-is-here.

Waterman, Shaun. "Fictitious Femme Fatale Fooled Cybersecurity." *The Washington Times*. 18 July 2010. http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity.

Ziezulewicz, Geoff. "ID Theft Surges Among US Troops in UK." *Stars and Stripes*. 18 November 2008. http://www.military.com/features/0,15240,179476,00.html.

ENDNOTES

1. According to Experian, a global information services company, social media sites have displaced search engines as the most visited sites in Singapore since September 2007.
2. "IDA Singapore: Infocomm Usage – Households and Individuals," Infocomm Development Authority, 14 September 2011, http://www.ida.gov.sg/Publications/20070822125451.aspx.
3. Singapore is ranked in the Top 10 worldwide in terms of Facebook penetration and Top 10 in Asia for the number of Twitter users. See "Facebook Statistics by Country," *SocialBakers*, 13 Sep 2011, http://www.socialbakers.com/facebook-statistics/?interval=last-week&orderBy=penetration# chart-intervals.
4. Ethan Bloch, "How are Mobile Phones Changing Social Media?" *FlowTown*, 30 March 2010, http://www.flowtown.com/blog/how-are-mobile-phones-changing-social-media?display=wide.
5. According to reports, the soldier updated his Facebook status saying, "on Wednesday, we clean up Qatanah, and on Thursday, God willing, we come home," in reference to a village near the West Bank city of Ramallah. The soldier's Facebook friends and fellow soldiers eventually turned him in. See Yaakov Katz, "Facebook Details Cancel IDF Raid," *Jerusalem Post*, 3 April 2010, http://www.jpost.com/Israel/Article.aspx?id=170156.
6. A similar incident occurred in 2008 when an IDF battalion commander was forced to cancel a mission due to Facebook posts made by a service member.
7. Murphy Kate, "Web Photos That Reveal Secrets, Like Where You Live," *New York Times*, 12 Aug 2010, http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html.
8. Geotagging is the process of adding geographical identification metadata to various media such as a geotagged photograph or video. Geotagging can help users find a wide variety of location-specific information. For instance, one can find images taken near a given location by entering latitude and longitude coordinates into a suitable image search engine.

9. Joesph L. Flatley, "US Army Connecting Soldiers to Digital Applications Program Putting Smartphones in Soldiers' Hands This February," *Engadget*, 14 December 2010, http://www.engadget.com/2010/12/14/us-army-connecting-soldiers-to-digital-applications-programs-put.

10. Joan Goodchild, "The Robin Sage Experiment: Fake Profile Fooled Military Intelligence, IT Security Pros," *Veterans Today*, 11 July 2010, http://www.veteranstoday.com/2010/07/11/the-robin-sage-experiment-fake-profile-fooled-military-intelligence-it-security-pros.

11. Shaun Waterman, "Fictitious Femme Fatale Fooled Cybersecurity," *The Washington Times*, 18 July 2010, http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity.

12. These contacts included executives at government entities such as the National Security Agency (NSA), Department of Defense (DOD), other military intelligence groups as well as friends coming from Global 500 corporations.

13. Elliott Fabrizio, "Dangers of Friending Strangers: the Robin Sage Experiment," *Armed with Science*, 21 July 2010, http://science.dodlive.mil/2010/07/21/the-dangers-of-friending-strangers-the-robin-sage-experiment/.

14. The classified information included active troops on deployment discussing their locations and what time helicopters were taking off for their missions.

15. In Israel, military intelligence officers were instructed to delete their Facebook and other social media accounts after it was discovered that some had been "friended" by Hezbollah operatives posing as Israeli women with the intention of gaining access to personal information.

16. Joseph Bonneau, Jonathan Anderson and George Danezis, "Prying Data out of a Social Network," 21 September 2011.

17. Danah Boyd, and Eszter Hargittai, "Facebook Privacy Settings: Who Cares?" *First Monday* 15, no. 8 (2010). The intention was to make the profile data available only for research purposes. However the data was deleted when Facebook threatened a lawsuit.

18. Jim Giles, "Data Sifted from Facebook Wiped After Legal Threats," *New Scientist*, 31 March 2010, http://www.newscientist.com/article/dn18721-data-sifted-from-facebook-wiped-after-legal-threats.html.

19. Half a year later, another security researcher wrote a similar script that managed to download 171 million public profile pages from Facebook and made the data freely available over the Internet.

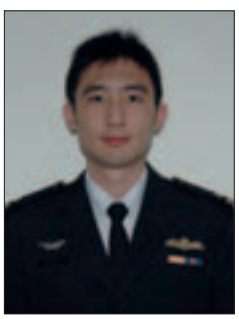
20. A post on a Al-Qaeda affiliated jihadist website instructed its followers to "quietly" gather intelligence about US military units, personnel as well as the family members, including which state they are from and their family situation. In addition, there were instructions to "monitor every website used by the personnel. ... and attempt to discover what is in these contacts."

21. Geoff Ziezulewicz, "ID Theft Surges Among US Troops in UK," *Stars and Stripes*, 18 November 2008, http://www.military.com/features/0,15240,179476,00.html.

22. "US Army Social Media Handbook is Here!" 20 January 2011, http://armylive.dodlive.mil/index.php/2011/01/u-s-army-social-media-handbook-is-here.

23. James Dunnigman, "Things Chinese Soldiers Are Not Allowed To Do," *Strategy Page*, 21 June 2011, http://www.strategypage.com/dls/articles/Things-Chinese-Soldiers-Are-Not-Allowed-To-Do-6-21-2011.asp.

24. Lucian Constantin, "Israeli Army to Block Social Networking over Security Concerns," *Softpedia*, 22 October 2010, http://news.softpedia.com/news/Israelian-Army-Blocks-Social-Networking-over-Security-Concerns-162515.shtml.



CPT Lee Hsiang Wei is a Helicopter Pilot by vocation and is presently an active pilot in 126 SQN. CPT Lee was a recipient of the SAF Overseas Scholarship in 2004. He holds a Master of Engineering and a Bachelor of Science in Electrical and Computer Engineering from Cornell University. CPT Lee was also the 2nd prize winner in the SAF Chief of Defence Force Essay Competition 2011/2012.