

Event Report 27-28 November 2014, Singapore

Centre of Excellence for National Security





Event Report

EMERGING TRENDS IN THE SOCIAL MEDIA DOMAIN: PERCEPTIONS, BEHAVIOURS, COMMUNICATION AND GOVERNANCE

Report on the workshop organised by:

Centre of Excellence for National Security (CENS) S. Rajaratnam School of International Studies (RSIS) Nanyang Technological University, Singapore

Supported by:

National Security Coordination Secretariat (NSCS) Prime Minister's Office, Singapore

Rapporteurs:

Priscilla Cabuyao, Joseph Franco, Caitríona H. Heinl, Navhat Nuraniyah, Nur Diyanah, Romain Quivooij, Jennifer Yang Hui and Yeap Su Yin

Editor:

Damien D. Cheong

The workshop adheres to a variation of the Chatham House Rule. Accordingly, beyond the speakers and presenters cited, no other attributions have been included in this report.

CONTENTS PAGE

1.	Executive Summary	3
2.	Opening Remarks	6
3.	Keynote Address: Too Much Digital Drama: A Better Approach to Online Discourse and Conflict	7
4.	Panel 1: Changing Perceptual Behaviours	9
5.	Panel 2: Public Trust in the Digital Age	14
6.	Panel 3: Case Studies 1	21
7.	Panel 4: Tools for Social Media Analysis	26
8.	Panel 5: Legal and Regulatory Frameworks	31
9.	Panel 6: Case Studies 2	36
10.	Dialogue Session: Evolving Government Communications in Singapore	41
11.	Workshop Agenda	42
12.	List of Speakers and Chairpersons	45
13.	About CENS, RSIS & NSCS	47

EXECUTIVE SUMMARY

Opening Remarks

Associate Professor Kumar Ramakrishna observed that it had become necessary to employ holistic approaches to deal with the challenges and opportunities created by social media, particularly in the areas of governance, public communication and the investigation of incidents. Ramakrishna observed how the rise of the Islamic State (IS) had once again raised the issue of social media to the top of policymakers' priorities. He emphasised that IS' continuing appeal resulted from the group's successes in both the online and offline realms. As such, it was necessary for states and other stakeholders to employ "integrated approaches" online and offline to deal with this threat. Ramakrishna also noted how social media analytics had grown in importance over the last few years. Recognition of the potential benefits of harnessing big data in the public and private sectors was testament to this. Ramakrishna concluded by urging participants to consider innovative ways to mesh theory with practice in order to leverage social media effectively.

Keynote Address: Too Much Digital Drama: A Better Approach to Online Discourse and Conflict

Andrea Weckerle began by giving an overview of the exponential growth of the World Wide Web from its esoteric roots to its current reach of around 2.5 billion people globally. Unfortunately, unbounded knowledge and connectivity appeared to have also brought about an epidemic of incivility and hostility in cyberspace. Online misbehaviour, Weckerle observed, was not limited to a select few, but noticeable in many ordinary Internet users as well. The Web's ability to anonymise the user has seemingly incentivised anti-social behaviour, with trolling becoming tantamount to Internet eugenics, that is, the shouting down and exclusion of other points of view. Weckerle also noted that conflicts that manifest online can result in negative outcomes in the real world, for instance, individuals driven to suicide and undermining of organisational productivity. Weckerle argued that a measured approach to online incivility was more effective than a reactionary/emotional one. She suggested that

emotional management and digital literacy were useful approaches to online misbehaviour and that sometimes, amicable resolutions were impossible to achieve despite one's best efforts.

The speakers examined different aspects of changing

Panel 1: Changing Perceptual Behaviours

perceptual behaviours in the online and offline environments. Associate Professor Ulrich Ecker observed that even after making corrections, misinformation could still influence a person's memory, reasoning and decision-making. Hence, a simple retraction of misinformation was ineffective. He suggested that when correcting misinformation, communicators should: (a) provide alternative explanations when retracting a myth; (b) focus on facts; (c) use simple language and graphs; (d) take recipients' worldview into account; (e) target the non-radical majority; and (f) preface misinformation with an 'Attention: Myth follows!' warning. Michael Ahn argued that the changing information environment had led to the diminishing effectiveness of traditional policy delivery systems. There was an increasing need, therefore, for "advertising,", "image-making" and persuading in communicating public policies. He suggested that using images and videos in public communication could: (a) induce participation; (b) create positive images of public policies; and (c) facilitate compliance with public policies. Finally, Professor David Chan discussed assumptions, analysis and action with regard to developments and approaches to social media in Singapore. With regard to assumptions, he said that it was essential to revisit assumptions about: (a) flaming vs framing; (b) vocal minority vs silent majority; (c) writer vs reader; (d) negative emotions vs negative mind-sets; (e) damage control vs strategic anticipation; (f) incident management vs recovery and resilience on social media; (f) rationality vs emotional. In relation to analysis, advances in sentiment analysis and the behavioural sciences allow useful insights to be gleaned from big data sets. Finally, the actions proposed included: (a) Principled Adaptive Leadership (PAL); (b) more effective public engagement; and (c) change achieving 'middleground' mind-set.

Panel 2: Public Trust in the Digital Age

This panel examined the issue of public trust in the digital age from three different practitioner perspectives. The first speaker, Associate Professor Eugene Tan, argued that trust was an essential prerequisite for meaningful engagement between the government and the citizenry. Trust-building was not necessarily about communicating better, but rather policies and administrative actions, especially unpopular/controversial ones that needed to be addressed. Tan opined that the new social identities observable in the social media domain could potentially challenge existing socio-political order(s). In addition, a social movement that was positioned as loyal to the nation and its people, but opposed to the government of the day could also emerge. The second speaker, Melvin Yuan, observed that social media had become integrated in many communication platforms, and had changed the traditional power structure between the communicator and the audience. As such, organisations needed to be more open, transparent, nimble, highlynetworked, collaborative and community-focussed in order to build public trust. The final speaker, Mr Vikram Nair, discussed how the government, through public sector agencies, was attempting to reach out to the public via various social media platforms. He argued that the humanising of communications was essential when communicating with the public today.

Panel 3: Case Studies 1

Through the use of different case studies, the panellists elaborated on some of the concepts discussed in the earlier panels. The first presenter, Jason Reifler, discussed the challenges of correcting misperceptions and the 'backfire effect', whereby attempts to correct misperceptions could actually result in further misperceptions. The second presenter, Strath Gordon, discussed Project Eyewatch, an online community policing concept by the New South Wales Police Force (NSWPF) that uses Facebook to combat crime and engage with the community. He underlined the value of this approach to not only increase efficiency in policing but also to build relationships between the NSWPF and local communities. Gordon also discussed how NSWPF had used social media during the recent anti-terror raids in Sydney. The third presenter, Hyunjin Seo, talked about the importance of visual propaganda in conflicts

between state and non-state actors that had appeared online. She examined twitter exchanges between the Israel Defence Forces (IDF) and Hamas' military branch during the conflict in November 2012, as well as Facebook posts between the Syrian government and the Syrian National Coalition (SNC).

Panel 4: Tools for Social Media Analysis

Several applications/tools for social media analytics were discussed in this panel. The first presenter, Carl Miller, spoke about new technologies and methods that could be used to study social media more efficiently e.g. natural language processing. He also discussed the implications and challenges for future research, analysis and policymaking in relation to social media science. The second speaker, Anne Kao, discussed the technical aspects of the TALISON (Tensor Analysis of Latent Interactions in Social Online Networks) software, which analyses Twitter data using tensors that are able to capture various parts of the content of online exchanges, takes into account the different forms of relationships and tracks the temporal dynamics and evolution of topics on social media. The final speaker, Brian Goode, introduced the audience to EMBERS (Early Model Based Event Recognition using Surrogates), a fully automated software that was capable of using data from open source indicators to forecast populationlevel events such as disease outbreaks, civil unrest, and election outcomes.

Panel 5: Legal and Regulatory Frameworks

The panellists discussed issues and challenges related to regulating social media analysis. Simon McKay talked about existing laws in the United Kingdom that regulate covert intelligence-gathering, and how regulation of open source intelligence-gathering was problematic. McKay suggested that in order to make the issue of open source and indeed covert intelligence-gathering less contentious, the simplification of legislation, clarification of a citizen's "constitutional" rights, review of objectives and methodology of covert policing resources, and an overall increase in transparency and accountability was needed. Benjamin Ang's presentation examined the statutory, legal and regulatory framework in Singapore that governs the use of data from social

media platforms for investigation, research or analysis. He also discussed the powers granted to the authorities under Singapore law in relation to the gathering and usage of such data. Professor Simon Chesterman shared his insights on regulating social media investigation and analysis. He argued that when developing a regulatory framework for social media investigation and analysis, the nature of the threat, the impact of emerging/new technologies and the influence of culture were important considerations.

Panel 6: Case Studies 2

The final panel of the workshop examined case studies that showed how social media is used for investigation, analysis and research. Rafael Lemaitre presented on the Federal Emergency Management Agency's (FEMA) use of metrics to evaluate the impact of its digital content/ messages online. He noted that it was fundamental to use the correct online platform for communication, the importance of connecting with the audience and the effectiveness of strong leadership in public communication. Professor Babak Akhgar discussed the features, advantages and challenges of open-source intelligence analysis. He also talked about the Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research's (CENTRIC) involvement in the Athena Project. The Project, led by West Yorkshire Police and funded by the European Commission, aims to utilise media communications and develop tools to enhance the ability of citizens and first responders in crisis situations. Christopher Church from the International Criminal Police Organization (INTERPOL) discussed digital forensics pertaining to social media applications on mobile devises. He looked at the evolution of social media on mobile devices, and how digital forensics is used to evidence data from mobile devices in criminal cases that involve social disturbances, sextortion and other illicit activities.

Dialogue Session: Evolving Government Communications in Singapore

Dr K U Menon began his presentation by giving a brief overview of the historical/political context that shaped government communications in post-independence Singapore. In the early days of the republic, it was held that Western norms regarding the media were not fully applicable to the local context. In addition, certain liberties, such as freedom of the press, were restricted for the sake of national development and the national interest. In contemporary times, however, this approach was increasingly being challenged, due in part to the fact that many Singaporeans were now living in a "postdeferential" age. Menon observed that the mainstream media in Singapore, contrary to popular belief, remained dominant despite the increasing popularity of online media. In relation to government communications, Menon argued that regular performance reviews as well as applying lessons learned and best practices to improve existing methods and approaches were essential. He also noted that recruiting talented individuals would be useful in light of the evolving communications landscape. In conclusion, Menon opined that good governance would remain an important measure of the government's performance.

OPENING REMARKS

Opening Remarks

Kumar Ramakrishna, Head, Centre of Excellence for National Security (CENS), RSIS



Kumar Ramakrishna

Associate Professor Kumar Ramakrishna

observed that it had become necessary to employ holistic approaches to deal with the challenges and opportunities created by social media. The inherent complexities and dynamics of the social media space required new ways of approaching the subject as well as determining how best to employ new investigative tools. This was envisaged to assist in the development of better communication strategies, as well as help improve overall investigation and analytical work in this field.

To illustrate, Ramakrishna remarked how the Islamic

State's (IS) rise to prominence was seemingly facilitated by the group's exploitation and leveraging of social media. Islamic State operatives appeared to have a clear grasp of the workings of different social media applications and platforms, were able to develop persuasive messages and able to reach their target audiences effectively. However, IS' appeal also stemmed from its offline triumphs, i.e. territorial conquests, which gave it tremendous credibility. Therefore, combatting IS should be carried out in both the offline and online realms.

The implication for practitioners and policymakers was that "integrated approaches" would be more effective in countering the influence of entities such as IS. And to that end, social media analytics was expected to be an important enabler. Social media analytics had grown in importance over the last few years as public and private sectors had recognised the potential benefits of harnessing big data.

As technology continues to improve and changes the way social media is used, Ramakrishna noted that regulatory, legal and overall governance issues would inevitably arise. The key challenge was to address these regulatory challenges satisfactorily without unduly hampering positive aspects of social media.

Ramakrishna concluded by urging participants to consider innovative ways to mesh theory with practice in order to leverage social media effectively.

KEYNOTE ADDRESS

Keynote Address: Too Much Digital Drama: A Better Approach to Online Discourse and Conflict

Andrea Weckerle, Founder, CiviliNation



Andrea Weckerle

Andrea Weckerle began her presentation by discussing the exponential growth of the World Wide Web, from its esoteric roots to its current reach to around 2.5 billion people. The ongoing evolution of the Web unfortunately, appears to have a dark side. The promise of unbounded knowledge and connectivity appeared to have brought along an "epidemic of incivility and hostility online". Misbehaviour in cyberspace appeared to be a widespread affliction as mainstream sites and applications are exploited through "Google bombs" and "Twitter bombs". Weckerle observed that almost every individual has experienced uncivil online discourse directly and/or indirectly.

The Web's anonymity incentivises anti-social behaviour. Instantaneous communication through the Web is also virtually free and takes away inhibitions. Benign triggers of anti-social behaviour can also include something as banal as boredom. Weckerle emphasised how trolling has become the most frequent example of uncivil behaviour online. Trolling taken to the extreme can be considered a form of Internet eugenics, as competing beliefs are shouted down and excluded. It was further stressed that while seemingly juvenile in nature, trolling could have major adverse consequences on individuals as well as organisations. For instance, trolling has been identified as a causal factor in several suicide cases, as targeted individuals were unable to seek respite

and redress from their cyber bullies. In relation to organisations, Weckerle argued that employee morale, productivity and organisational reputation could suffer from online misbehaviour.

There were also negative ramifications to society at large. Online conflicts inadvertently reward the loudest and most aggressive voices, and in this sort of environment, rumours can easily become 'facts'. In addition, a two-tiered system of social interaction is fostered as online spaces are used as an avenue for abusive speech, which ordinarily would have been frowned upon in the offline world. As a result, online misbehaviour creates opportunities for sanctioned social abuses and threatens meaningful norms such as freedom of speech.

Weckerle argued that a more dispassionate approach, as opposed to a reactionary one, was needed to deal with online miscreants. She noted that online culture is continually constructed by its users, who are not simply passive recipients. As such, online users needed to be more calibrated in their emotional management so as to toughen themselves against trolls and avoid taking offence easily. In addition, users should increase their digital literacy and be aware of the risks and dangers when engaging others in online spaces. Individuals should also be aware of their trigger points so that they can better deal with attacks on their character (ad hominem attacks).

When dealing with problematic engagements online, Weckerle urged the audience to first consider if responding was even worth the effort since even a constructive response would fail to dissuade trolls as they are often not amenable to conflict resolution and/ or constructive dialogue. If a response is needed, then the individual must deliberately think through when and how to frame the response.

Weckerle also discussed the role of online bystanders and their tacit ability to sway online conflict away from the actual belligerents. Emotional contagion was a very real phenomenon in massive social media networks, which further underscored the need for deliberate responses against uncivil online behaviour.

Discussion

A participant wanted to know if a legal definition of 'trolls' and 'trolling' was possible. Weckerle opined that there were various legal definitions around the world that were used to cover abusive behaviour online, and the breadth of these definitions did create inconsistencies.

Another participant asked for an elaboration on the psychological profile of trolls. Weckerle responded that in general trolls were individuals who attack other online users simply for sport. There were also many different categories of trolls (e.g. spamming, flaming, hit-and-run, kooks, etc.). However, recent studies had revealed certain psychological traits that were common in trolls such as sadistic and narcissistic tendencies and low levels of empathy for others.

PANEL 1:

CHANGING PERCEPTUAL BEHAVIOURS

Misinformation and its Correction in the Social Media Domain

Ullrich Ecker, Associate Professor and Research Fellow of the Australian Research Council, School of Psychology, The University of Western Australia



Ullrich Ecker

Associate Professor Ullrich Ecker's presentation discussed four main points: (a) how misinformation was disseminated in the society; (b) the cognitive factors that render misinformation resistant to correction; (c) misinformation's effect on an individual's reasoning; and (d) recommendations to reduce the impacts of misinformation.

In general, there were two kinds of misinformation phenomenon: First, the post-event effect whereby individuals initially receive valid information about an event but alter their memories following exposure to misinformation after the event. Second, the continued effect, whereby incorrect information is spread initially but subsequently retracted and corrected. Ecker's presentation focused on the latter.

Misinformation can be disseminated either inadvertently or deliberately through traditional and new media, rumours and fiction. With regard to traditional media, misinformation could inadvertently spread due to the pressure of competition and the seeming obsession with balanced coverage even when balance is absent. Social media, too, has become rife with misinformation due in part to the fact that

many posts try to elicit emotional responses or are themselves emotional responses with little or no factchecking.

There are also inherent characteristics in an in individual's memory that make people vulnerable to misinformation. The reconstructive nature of memories allows fault memories to be easily implanted on people's minds. Furthermore, people's desire for a complete mental map of the world make them believe in even the most blatant, deliberate conspiracy theories as long as they offer complete answers. In the current information age, people simply have limited resources to thoroughly evaluate all evidence, so they turn to heuristic reasoning such as filtering information that fits in with their prior belief or with the opinions of trusted others.

Based on his study of post-retraction reliance on misinformation, Ecker noted that belief in misinformation cannot be fully eliminated, it can only be reduced. Misinformation can have long lasting effects on people's memories, reasoning and decision making even after its retraction. An example cited was the myth about the dangers of vaccines that had resulted in a significant reduction in the vaccination rate in the United Kingdom. It emerged that even after the myth was refuted, retracted and corrected, there were many people who still believed it. This showed that simple retraction of misinformation is inefficient because memories cannot simply be erased. Debunking misinformation requires better, more plausible alternative information to fill in the gap left by the retraction. The study also showed that trustworthiness of the source rather than expertise could significantly affect the effectiveness of retraction and correction (a point that underscores the value of social media influencers).

It was important to be mindful that retraction of misinformation could result in several negative outcomes. Firstly, the familiarity backfire effect, where people remember the misinformation due to its constant repetition as attempts are made to retract/ correct it. Hence, it was important to avoid unnecessary repetition of misinformation, and to always start any retraction attempts with facts in order to set the right frame of mind.

Secondly, the worldview backfire effect could occur in people who have strong attitudes and beliefs on a topic. Retraction is effective only when this is congruent with the individual's worldview; otherwise it only increases his/her belief in the invalid claim. This is because people tend to counter-argue inconvenient retraction. To avoid this, the message can be framed to affirm a particular worldview. For instance, businesses are more likely to accept corporate social responsibility if it is framed as a potential source of business opportunities rather than as a set of regulations.

In closing, Ecker stressed the importance of focusing on the undecided majority instead of the opinionated vocal minority because the former are more receptive to information correction than the latter.

Effective Public Policy Communication in the Age of Information Overload – The Role of Imagery on Citizen Perception and Compliance of Public Policy Michael J. Ahn, Assistant Professor, Department of Public Policy and Public Affairs, University of Massachusetts, Boston



Michael J. Ahn

Michael Ahn's presentation focussed on the changes in the communication environment particularly in terms of information overload and the emergence of imagery communication. He also looked at how such changes affected the effectiveness of public policy communication.

The rapid growth of Internet users and traffic has resulted in information overload, which in turn, has prompted the growth of imagery communication. This is because in a sea of textual and verbal information, visual images are effective attention-grabbers.

Psychology studies have shown that filtering information is central to a human's decision-making abilities. The availability of too much information slows this process down and impairs the filtering capacity. Visual information can help overcome such limitations in four ways: (a) the information is condensed hence enabling faster processing; (b) more stickiness and memorability; (c) higher reachability as pictures and videos are more vivid and relatable; and (d) images have more emotional appeal compared to texts.

In this context, visual communication arguably offers more benefits to policy communication in terms of inducing public participation and compliance. For instance, in the case of electric waste management, instead of explaining the policy rationale in lengthy documents, communicators could show images of environmental degradation resulting from electric waste. Such images can be more effective in appealing to citizens' emotions and motivate them to take action.

Ahn argued that there is currently a mismatch between government's approach to public communication and the communication needs of this generation of individuals. Information overload has changed the way people react to public information – peoples' attention spans are getting shorter and they became more attracted to emotionally appealing videos and images. However, most governments still use traditional, top-down communication that present objective facts and communicate messages that seem devoid of emotion.

The diminishing effectiveness of traditional policy communication was highlighted in the case of the 2008 US beef protest in South Korea. Despite the presence of other factors such as heightened disappointment with the government, the massive protest was directly triggered by a widely-watched documentary that suggested beef imported from the US may be contaminated with mad cow disease.

The government attempted to correct the misperception by releasing objective facts and

data about mad cow disease, and employing experts to disseminate such facts through the media. The documentary maker was also asked to apologise for giving inaccurate information on the disease. However, such efforts only increased public confusion as many found it difficult to determine the truth from myth, and consequently many ended up believing the original misinformation (this outcome underscores Ullrich Ecker's point about the familiarity backfire effect). Levels of public trust significantly decreased as a result.

In conclusion, Ahn argued that to achieve more effective policy communication, the government should not only harness the benefits of visual communication but also alter their overall approach to policy communication. The emphasis should extend beyond informing the public to proactively shaping their first impressions of a particular policy. Ahn also concluded that there is an increasing need for advertising and image-making of public policies.

Understanding Social Media in Singapore: Assumptions, Analyses, Actions

David Chan, Lee Kuan Yew Fellow and Professor of Psychology, Director, Behavioural Sciences Institute, Singapore Management University



David Chan

Professor David Chan's discussion focussed on three areas of inquiry: (a) emerging issues in the social media domain in the Singapore context; (b) challenging

old assumptions regarding social media; and (c) new approaches to better deal with social issues especially in the online realm.

Chan began by pointing out that issues that are hotly discussed and debated in the social media space in Singapore occur in specific socio-political settings and evolve with on-going socio-political changes.

He observed that social media did pose some challenges to the government. For one, the socially uniting influence of social media can enable collective action, but the outcomes can be either positive or negative. For instance, promoting charitable events and activities can be regarded as a positive outcome whereas inciting people to carry out hate crimes can be classified as a negative outcome.

Perhaps one of the biggest challenges posed by social media is that its ever-increasing connectivity and immediacy often requires immediate policy solutions, which the existing hierarchical policy-making structure often cannot cope with. To respond efficiently and timely, policy makers need to be equipped with pattern-recognition skills in addition to traditional analytical skills.

Widely-held assumptions about netizens may have to be re-evaluated. For example, the assumption that social media serves as an echo chamber for the vocal minority may have led to the dismissing of legitimate social concerns. Also, the distinction between vocal minority and silent majority may not be wholly applicable in the Singapore context given that vocal minorities may at times be highlighting issues that affect the silent majority a well. Furthermore, assumptions about human behaviour need to be relooked as well. It is often assumed that emotion and rationality are mutually exclusive; however, they are actually intertwined.1 As such, social behavioural scientists and technological experts should be engaged collaboratively to generate more accurate analyses of social media data.

Chan further suggested two courses of action to

A good informative piece on the topic: http://www.fastcocreate.com/1682962/the-end-of-rational-vs-emotional-how-both-logic-and-feeling-play-key-roles-in-marketing-and-

encourage civility in the social media domain without limiting critical voices. Firstly, the government should go beyond a legalistic approach and work more on public education to promote good conduct online. Whilst important, the rule of law is not the only way to induce compliance. The fear that online anonymity leads to uncivil behaviour has overlooked that fact that most people are capable of learning and internalising values that can guide their behaviour both online and offline.

Secondly, the government needs to change its tensional, trade-off mind-set when framing policy issues. For instance, the concept of "democracy of deeds" promoted by the government has come at the expense of "democracy of voices" with implications observable in the social media domain. The talk-less-do-more model of democracy means that critical voices are not encouraged and even considered counterproductive. In fact, doing and talking reinforce each other. Emotion drives people to speak up and subsequently discuss rational, actionable solutions. As such, a unifying approach should instead be promoted because solutions in community can be only found when both rationality and emotion are equally appreciated. Finally, Chan concluded that "democracy of deeds and voices"2 should be the basic principle in managing socio-political issues offline and online.

Discussion

A participant asked why some people would still believe in misinformation even after being given the correct information. A speaker replied that such individuals were inclined to do so due in part to their personal prejudices, grievances, ideology and so on. It was therefore unrealistic to attempt to eradicate misinformation completely from peoples' minds. However, it was possible to nudge individuals to question the misinformation by: (a) highlighting factual evidence; (b) creating suspicions as to the real motives behind the claim; or (c) providing the context to the claim such as the source's organisational background.

Here, scepticism was the key to minimise the ill-effects of misinformation.

It was also noted that often, the most effective way of correcting misinformation was the passage of time. Time enables a person to cool down, which in turn, results in more objective reasoning. It also helps in debunking myths because new evidence might surface to further disprove the original claim.

The trustworthiness and/or gravitas of the individual correcting the misinformation were also important. This underscored the importance of selecting the appropriate spokesperson/spokespeople to represent an organisation especially during crises.

With regard to public and policy communication, a participant observed that the speed of dissemination of rumours and other misinformation on social media may actually be too fast for governments and practitioners to react appropriately in time. This could compromise the process of correcting the misinformation, especially when comprehensive data and statistics are involved (in light of the time needed to put together such information) as well as adversely affect public perceptions. It was suggested that the government work more closely with representatives on the ground to build trust and goodwill overall.

In terms of how to craft messages more effectively, a speaker suggested that communicators should 'make things as simple as possible, but not simpler'. Information and visuals should be easy to understand and relatable to the different sections of the society to ensure greater retention. Also, the accuracy of the facts must not be compromised, and the government should not release information hastily, but only when all the facts have been reasonably ascertained.

In relation to strategies to deal with target audiences, a speaker stressed that communicators should be strategic, attentive and engaging in an effort to build overall trust. Communicators should also carry out research on the different segments of the target audience to ascertain their information needs, tailor

² See David Chan, 'Democracy of Deeds and Voices', *Straits Times*, (7 June 2014). Available: http://www.straitstimes.com/news/opinion/invitation/story/democracy-deeds-and-voices-20140607

messages accordingly, and use the most appropriate means/medium of disseminating the message (here a crisis communication plan would arguably be extremely useful). In doing so, the overall time taken for the government to respond would likely be reduced. Interagency coordination would also help in this endeavour.

A participant enquired as to whether education as opposed to harsher penalties was more effective in regulating problematic online behaviour. A speaker opined that there had been an overemphasis on negative behaviour, and as a result, the focus was on developing more regulatory structures and/or introducing stiffer penalties to address the issue. However, there was also a lot of positive behaviour noticeable online too. As such, a possible strategy might be to leverage positive experiences of others to educate and correct negative behaviour rather than penalising/punishing individuals. Although there were many arguments for and against the employment of hard and soft approaches to correct online misbehaviour, it was important to approach the issue from a multi-dimensional angle.

Ensuring that individuals were equipped with the right skills and knowledge to deal with online misbehaviour was also important. Hence, digital media literacy needed to be constantly reviewed. In the Singapore context, the focus has traditionally been on self-protection and cyber bullying. However, Singapore would need a more systematic and comprehensive social media master plan to deal with and anticipate emerging problems. This plan would naturally benefit from public consultation and input.

Another participant wanted to know if the government should be proactive in online debates about localised issues. A speaker replied that there were several advantages of doing so including being able to redirect the focus of discussions, and/or manage debates that may cause social disturbances. It was suggested that 'credible voices' and/or social media influencers be employed to assist in this endeavour. It was also important for the government to manage its image and reputation on and offline effectively.

A participant asked if contextual differences were important in attempting to change perceptual behaviours. A speaker suggested that governments should not treat societies and/or communities as homogenous but if possible, carefully assess the different needs/issues/complaints etc. of the different groups of people so that the issues could be dealt with properly. It is by doing so that trust can also be nurtured. This suggests a need for governments to be more attentive to how they approach issues and policies especially contentious ones.

PANEL 2:

PUBLIC TRUST IN THE DIGITAL AGE

Enhancing Trust in the Government – Views from a former Nominated Member of Parliament

Eugene Tan, Associate Professor of Law, Co-Director, SMU Centre for Scholars' Development, Singapore Management University



Eugene Tan

Associate Professor Eugene Tan began his presentation by explaining how, globally, social media and the Internet had become enablers of the masses over the last few years. Individuals were now empowered to challenge hierarchies and authority through various new platforms on the Internet and their hand-held devices. He cited the Arab spring and exposes carried out by citizen journalism as examples of this.

In Singapore, too, the Internet and social media were perceived by some as avenues to overcome restrictions on freedoms of expression and association. The development of new social identities could potentially challenge the existing socio-political order(s), especially when individuals, who are strongly opposed to the status quo, form groups online. A possible outcome is the emergence of a social movement that is positioned as loyal to the nation and its people, but opposed to the government of the day.

In relation to trust, A/P Tan argued that trust is the prerequisite for meaningful engagement between government and the citizenry. It also helps to ensure that close-mindedness does not prevail. Trust-building

was not necessarily about communicating better, but rather addressing and/or improving policies and administrative actions, especially unpopular/controversial ones such as the population white paper. A/P Tan acknowledged that the government had taken steps to improve its outreach and engagement through initiatives like the Our Singapore Conversation and the introduction of the Pioneer Generation Package, as well as the increased usage of social media platforms.

A/P Tan argued that there were several issues that would have an impact on trust-building efforts: (a) the increasingly competitive political landscape in Singapore; (b) the gradual withering of one-party dominance; (c) related governance issues; (d) operating within a (contested) framework where party, government and state are often conflated; and (e) the shift from mainstream media to new media.

He made several suggestions on how trust-building could be improved: (a) it was necessary to tap bottom-up input to forge political buy-in, and that would help in trust and confidence-building in light of the evolving governance challenges; (b) there was a need to focus on values and social issues; (c) debunking myths, correcting misinformation and misperceptions were also essential; and (d) sustained engagement should be attempted, and be based on principles and reason, with a view to engage, understand and persuade one's interlocutor.

To sum up, A/P Tan made the following observations: (a) it is difficult to control the 'imagined communities' of netizens; (b) social media may adversely affect critical thinking in the long run and result in 'echo chamber' effects; (c) increased participation online does not necessarily mean action offline; (d) there is an ongoing recalibration of the relationship between the government and citizens; (e) the patriarchal and top-down approach to government is waning; (f) there is a need for a quickened pace of engagement; (g) values and motivations matter in government communications; (h) people's ideas about the proper role of government communications matter

tremendously and (i) government communications succeed not so much by nudging people to make a real sacrifice but rather getting people to do things when they are not so motivated enough to make a real sacrifice.

Increasing Public Trust in the Social Media Age – Views from a Senior Communications Practitioner

Melvin Yuan, Founder/Director, Omnifluence



Melvin Yuan

The second speaker, **Melvin Yuan**, condensed his presentation into ten professional observations made on the topic from his experience working with several private sector companies:

The Social Technographics Ladder

Social Technographics classifies people according to how they use social technologies.

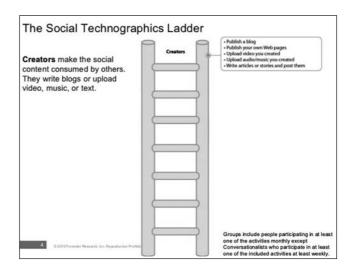
Forrester can quantify the number of online consumers within these groups using our global Technographics® consumer surveys.

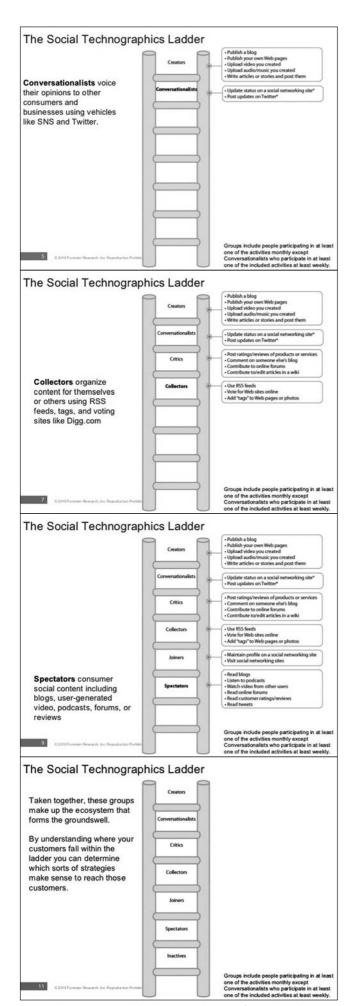
Collectors

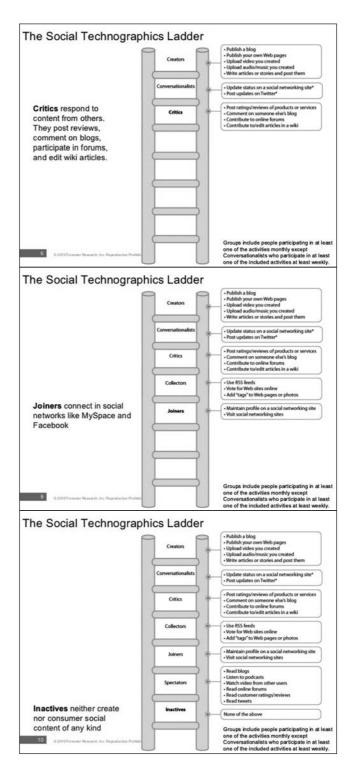
Spectators

Groups include people participating in at least one of the activities monthly except Conversationalists who participate in at least one of the included activities at least weekly.

- (1) There is no such thing as social media these days as social media has become quite integrated in many IT and communication platforms. Hence, social media activity is not unique but must be integrated into the organisation's activities.
- (2) Social media is about the disruption of traditional power structures between the communicator and the audience. This suggests that the traditional business and communication models are outdated. It is now not about managing a set of communication platforms well, but rather about relationship management between government and citizens, business and consumer and so on. Leadership styles and culture must therefore change.
- (3) Organisations must strive to be highly networked, collaborative, nimble, open, transparent, and community-focussed in the digital age.
- (4) The existence and persistence of behavioural and cultural diversity necessitates engagement to be sensitive to these differences. To better understand the differences between how people behave on and offline, Yuan recommended the use of the Social Technographics tool by Forrester (http://empowered.forrester.com/tool_consumer.html):







Source: http://www.slideshare.net/jberno1ff/social-technographics-defined-2010

Learning more about one's target audience would certainly help with communication efforts.

- (5) Leveraging the super human, that is, the social media influencer. Yuan suggested that organisations empower more people within the organisation, especially the more passionate ones, to act as influencers.
- (6) The re-emergence of self-organising tribes online means that traditional one-to-many communications are less effective nowadays. Yuan suggested that organisations identify these tribes and attempt to actively participate in the conversation (e.g.: http://www.marketing-interactive.com/scoot-turns-sgag-drama-into-promotion/)
- (7) Dealing effectively with large volumes of data requires better filtering and data analysis. Organisations should therefore include data analysts and researchers in their communications team.
- (8) There is a need for 'story tellers' in a communications group to create affinity through emotive stories, empathy and humanising experiences. [rapporteur's input: see for example the commercial 'Funeral', commissioned by Families for Life, Ministry for Social and Family Development, Singapore: https://www.youtube.com/watch?v=s2XLZsiCBsA].
- (9) Total control over the message, channels and negative comments is unrealistic. Practitioners should instead focus on doing their jobs well (performance) so that the public would be more sympathetic and indeed empathetic to shortcomings.
- (10) Organisations should think collaboratively and leverage the 'wisdom of the crowds' to improve engagement.

Enhancing Trust in the Government

Mr Vikram Nair, MP, Sembawang GRC and Vice-Chairman of Sembawang Town Council



Vikram Nair

Mr Vikram Nair began his presentation by discussing the evolution of social media and the Internet to demonstrate the phenomenal growth of this communication platform over the last four decades. Social media applications as well as the number of users globally were expected to continue to grow exponentially in the future. As such, social media had become a sort of "electronic second life" for many.

The proliferation of social media, while generating many positive outcomes such as facilitating communication between people across the globe and mobilising people to take positive actions, could also be used for negative purposes. These included revolutions; riots; identity theft; defamation and stalking.

Mr Nair observed that governments, too, were attempting to reach out to the public via various social media platforms. The creation of personal Twitter accounts and Facebook pages has found favour among many politicians and government agencies worldwide. This has enabled a less formal way of communicating and allows the politician and/or agency to appear more personable.

Several examples from Singapore were cited: (a) PM Lee Hsien Loong's Twitter account; (b) National Development Minister Khaw Boon Wan's blog which "is for Minister Khaw to share some of his thoughts, considerations, and suggestions on issues related to MND matters in Singapore"; (c) the LTA Facebook page; (d) REACH Facebook page, which "gather[s]

and gauge[s] ground sentiment, reach[es] out and engage[s] citizens and promote[s] active citizenry"; (e) MOE Twitter account; and (f) GOV.sg Facebook page, which publicises the "latest policy announcements, information and news on Singapore". He also argued that the humanising of communications was essential when communicating with the public today.

Finally, Mr Nair outlined several laws that pertained to social media namely: (a) Computer Misuse and Cybersecurity Act (CMCA); (b) Undesirable Publications Act; (c) Protection from Harassment Act 2014; (d) Defamation Act and (e) Penal Code.

Discussion

A participant asked if there were other better methods of assessing whether an organisation/individual's social media outreach was effective apart from analysing 'likes' and 'followers'. A speaker replied that in the area of communications, there is much room for improvement, especially in terms of tapping employees' abilities to act as brand ambassadors within their social networks. The problem of current organisations is that they are still basing their communications approach on an industrial age model when we are in fact in the digital/information age.

A typical organisation still operates with a few individuals responsible for corporate communications including social media outreach, and then measuring/evaluating the impact and effects of those activities. However the digital age actually enables every employee to use social technology in a way that improves the overall image of organisations. For example, Google uses new, more social way of operating whereby every entity can be responsible for innovation. If all members of the organisation could be counted on to influence their peers there would be a multiplier effect that would greatly elevate the corporate branding. One thing that organisations fail to realise is that it is not communication that has changed but it is the way that people communicate and behave. Therefore, with social media, there are actually more potential ways to problem-solve [editor's input: e.g. crowd-sourcing]. Organisations, however, seem to have problems meeting the fast-pace interaction between people that occurs in the digital age. Therefore, there needs

to be a radical shift in management mind-set to view organisations not as hierarchies but as networks; only then will workers be empowered and organisations more adapt to tackle modern communication problems.

Another participant enquired if there was a difference in the way private companies create trust with customers as opposed to the way government create trust with the citizenry. For example, some companies tend to want to position themselves as youthful, cool and hip but this approach may not be applicable to the government. A speaker replied that people do not necessarily trust organisations and brands easily as they do people. It is actually easier to build relationships between humans as opposed to building relationships with corporations. Hence, if the people behind and/ or working for the corporation are seen by the public to be trustworthy, then the corporation itself will be seen to be trustworthy. But today it seems that many employees are not empowered to act unilaterally and make their own decisions, so trust-building has become challenging, especially when scandals, missteps or genuine mistakes get amplified on social media. The government, too, can apply this strategy and in so doing help trust-building. [Editor's input: For example: (i) compassionate parking warden

(http://singaporeseen.stomp.com.sg/singaporeseen/get-inspired/parking-warden-give-chanes-to-errant-driver-in-spirit-of-chinese-new-year); and (ii) swift responses and active problem-solving by LTA (http://smallwheelsbigsmile.blogspot.sg/2014/08/feedback-to-lta-and-it-worked.html)].

A participant enquired if there were situations where it would be better not to do anything at all, as it was likely that a response would exacerbate the issue, crisis and/or situation, and if the speaker could discuss an example from the public sector. A speaker responded that a public sector example did not spring to mind. However, in the private sector, he has noticed that a crisis is identified too early and too prematurely. As almost all of the communications work on and offline is handled by a communications team, of which the social media team is a part of, many of them don't have the data and the analytical skills to properly determine if an issue will turn into a full-blown crisis. Hence, they cannot determine if responding or not responding is the correct strategy to de-escalate the situation.

A participant enquired if there were strategies to prevent incorrect information and/or misinformation from being disseminated. A speaker suggested that the right kind of training, workflows and processes were needed. Many organisations, including some public sector ones, operated where there were communications teams of about five people handling internal stakeholders of around 1000 people. In reality, they were probably dealing with about 100 people within the organisation, helping them with crafting emails, events, announcements, or policies. Imagine if a hundred people in the organisation were permitted to craft their own messages, taught the best way to craft these messages, and to communicate effectively with the organisation's external audience. This would reduce the likelihood of misinformation and incorrect information from being disseminated.

A participant wanted to know how the People's Action Party's (PAP) approach to social media had changed since the Singapore 2011 General Elections. Prior to the elections, even though the PAP had prided itself as a party that could provide solutions to the problems most people faced, not enough was done to communicate that, i.e. policies were not effectively communicated. This was one of the major changes after the election. And even though some of the older generation of PAP MPs may not have social media accounts, they still have ways to engage and reach out to their constituents.

One other observation was that prior to the 2011 elections, many individuals seemed to use social media as a platform to challenge and criticise the PAP and the government [rapporteur's input: see research by IPS http://lkyspp.nus.edu.sg/wp-content/uploads/2013/06/pa_TTHAM_Subverting-Seriousness_AMIC_July-2008.pdf]. Nowadays, although social media is still used in that way, many people are also using it to stay informed, find out more about issues, activities, government initiatives, offer suggestions/inputs and engage with the government. As mentioned in the presentation, the government, too, has taken steps to use social media as one of the ways to engage the citizenry.

The speaker noted that it was important to enhance public trust through dialogues and engagement. However, it should be noted that not everyone was willing to come forward to engage in dialogue as well. There are some citizens who want to be heard but feel uncomfortable about speaking up.

A participant wanted to know what the role of traditional media, particularly the Straits Times/broadsheets, was vis-à-vis new media. A speaker replied that the relationship between traditional media and new media was an interesting one. Social media could never replace the traditional news outlets. This was because someone actually needs to do the reporting, that is, someone needs to go to the site to write the story down. The story will be commented on and shared on social media, but social media does not seem to have the capability to be a primary news generator. Primary news would still have to come from journalists who do the reporting. Without traditional media, social media would not have something to bite on, there would be nothing much to talk about. There is a possibility that traditional media would get smaller - a trend noticeable worldwide. However, whether traditional news outlets in Singapore published in print, move completely over to digital, or continue to straddle both, as is currently the case, remains to be seen.

A participant wanted to know about the origins of the Protection from Harassment Act 2014 and how harassment was defined. A speaker replied that feedback from a wide range of sources prompted the enactment of the legislation. The definition of 'harassment' is broadly-defined and hence, any activity that could potentially distress a person, and done with the knowledge that it would distress the person is deemed harassment. The Act doesn't only focus on cyber-bullying, but covers all forms of harassment including stalking.

A participant wanted a speaker to elaborate on a statement he had made in parliament that "what is not said is as important as what was said". The speaker replied that if something is important to the citizens, they would bring it up somehow. Just because only a few voices are heard on the subject doesn't mean that more people are not concerned. As such, more dialogue is necessary, and concerns must be looked into, as silence on an issue could provoke harmful speculation. Increasingly, government communications must be able to deal with challenging and sometimes controversial issues. Decision makers should also not

be afraid to approach inconvenient truths, and should realise that there are possibilities of building trust through dealing with difficult issues.

A participant enquired if government outreach initiatives were successful? A speaker replied that after the 2011 General Elections, citizens were expecting the government to deliver on their promise of increased engagement and consultation. This requires a lot of effort, and the question is whether such efforts were generating tangible positive outcomes.

A participant wanted to know if the law should make a distinction between the online and offline realms. A speaker replied that in the context of Singapore, the law is fairly clear: it does not differentiate between the online and offline worlds. The intention of not doing so is to underscore the expectation that the same set of rules would apply in both the on and offline worlds. However, in the online world, the rules of engagement

are unfortunately quite different from the offline world. There is merit in attempting to try and have both worlds converge in terms of the rules of engagement, if not the World Wide Web might just become the Wild, Wild West. There is also an appreciation that the online world is a very powerful communication platform, perhaps a lot more effective in terms of spreading information or misinformation compared to the mainstream media. Nevertheless, the question remains as to whether people want the rules of engagement for the on and offline realms to be the same. That is why the news of the prime minister suing a blogger for comments made online (which are certainly defamatory) took many by surprise.

A participant wanted to know if silence was golden in some situations. A speaker replied that although there was a risk of exacerbating an issue if one discusses it, engagement was necessary as silence could be misperceived and lead to a negative outcome.

PANEL 3:

CASE STUDIES 1

Correcting Misperceptions: What Works

Jason Reifler, Senior Lecturer of Politics, University of Exeter



Jason Reifler

Jason Reifler's presentation discussed strategies to correct misperceptions that were based on past psychological studies carried out with Brendan Nyhan. He observed that misperceptions distort political discourse, debate and policy-decision making thereby adversely affecting an individual's understanding of political matters.

A distinction was made between 'uninformed' and 'misinformed' people, with the latter defined as individuals whose beliefs are thought to be correct but are in actuality false or unsubstantiated. Several causal factors of misperceptions were listed: (a) information deficit stemming from the absence of good-quality and/or sources of information; (b) active counterarguing may lead some individuals to entrench themselves in their positions; (c) cognitive biases and memory failure; (d) availability of alternative sources of information (information-overload); (e) accurate information not presented in a convincing format; and (f) the psychological discomfort caused to an individual by accurate information especially when such information significantly contradicted an individual's pre-existing beliefs.

Reifler discussed two experiments that examined the link between information, self-esteem and interpretation in order to find out new methods of correcting misperceptions. The first related to US troop withdrawals in Iraq and the other involved the state of employment under the Obama administration. The results demonstrated that self-affirmation and delivering factual information in a more appealing/persuasive manner were shown to be effective in reducing misperceptions as well as highlighted the connection between an individual's sense of self and the way he/she interprets events and situations.

Applying these findings to a political context, Reifler discussed another study that involved the creation of a fictitious politician who was subjected to accusations of corruption. Based solely on such allegations, opinions on this hypothetical character were largely unfavourable. However, the provision of a straight denial and a coherent counter-narrative subsequently improved their perceptions. Yet another study found that fact-checking might actually deter individuals from disseminating misinformation if their reputations were at stake.

There were, of course, challenges associated with attempting to correct misperceptions. Reifler discussed the outcome of a study aimed at correcting the misperception that that was a causal link between the vaccine for measles, mumps and rubella (MMR) and autism. The study showed that the perceptions of people with pre-oriented beliefs were unlikely to change, regardless of the correction information presented to them.

From this study, misinformation can be characterised as a dual issue of demand and supply, whereby most individuals seem prone to favour misinformation as long as it supports their beliefs, and tend also to deny the validity of contradictory information. On the supply side, misinformation can be a useful tactic for political communication.

Enhancing Public Confidence in the NSW Police Force – Project Eyewatch

Strath Gordon, Director, Public Affairs, New South Wales Police Force



Strath Gordon

Strath Gordon's presentation focused on Project Eyewatch, an initiative that aimed to improve the New South Wales Police Force's (NSWPF) communication and outreach with the public, as well as social media strategies used during crises such as counter-terrorism operations.

Although traditional media such as print, radio and text messages were the primary methods used in the past by the NSWPF to engage the public, social media had proven to be a more suitable platform in light of the density of the population and the diversity of local security environments in the Australian state of New South Wales.

The overarching strategy of the NSWPF is to work in tandem with the community to deal with crime and community safety issues. It has been demonstrated that through such partnership, and in particular, through the use of information provided by the public, crime rates in major categories have dropped over the years.

In terms of communication, the NSWPF hopes to highlight the benefits of such cooperation in order to continue building confidence, trust and goodwill. Traditionally, the NSWPF relied mainly on traditional news media to communicate with the public. Although effective, it could often be slow, biased and one directional (top-down communication). The NSWPF therefore want to leverage IT and communication

technology to reach the community through more effective methods.

The NSWPF started using two social media platforms in 2009 (Twitter and YouTube), and subsequently adopted Facebook the following year. Facebook became the most popular platform and proved to be ideal for interactive two-way communication. Facebook is used to publicise arrests, appeal for information on wanted or missing persons, provide updates on traffic and crowd information during major events and provide positive stories on the various aspects of policing.

Gordon observed that the social media outreach initiatives had produced good results, particularly in terms of dealing with crime, finding missing people, generating awareness about police work and enhancing service provision. Among the key lessons learned included the need for: (a) specific policies to address how social media accounts of NSWPF personnel should be managed; (b) policies to deal with risk management, disclosure of confidential information and damage to the creditability of the organisation; and (c) efficient monitoring and evaluation of social media sites. Operationally and administratively, there was a need to: (a) create an internal social media committee to represent all key internal stakeholders; (b) have centralised governance, that is, authorisation of profiles/authentication processes for the NSWPF social media presence; (c) develop social management tools; and (d) build relationships with external stakeholders. These issues were summarily addressed with the introduction of comprehensive social media policies that governed official and personal use.

Among the future developments with regard to improving Project Eyewatch was the design and implementation of an effective crime reporting mechanism online. Also, attempting to keep the public sufficiently engaged was expected to be a persistent challenge.

In demonstrating how the NSWPF maintained its control and monopoly of information during a crisis, Gordon discussed the communication strategies used in the counter-terrorism raids in Sydney and Brisbane in September 2014. The NSWPF was the first to break the news issuing a tweet when the operation

commenced. It then continued to provide updates on Twitter including images, and moved quickly to debunk misinformation/rumours. This enabled them to shape the narrative and minimise rumour-mongering.

In sum, Gordon argued that content management, in particular, providing consistent updated information online, was a crucial activity which defined the 'Eyewatch brand', and had positively affected the reputation of the NSWPF. Because of the evolving nature of the Web and social networks, regular evaluation periods have to be set up in order to keep pace with the requirements of technological developments.

Visual Propaganda in the Age of Social Media

Hyunjin Seo, Assistant Professor and Docking Faculty Scholar, William Allen White School of Journalism and Mass Communications, University of Kansas



Hyunjin Seo

Hyunjin Seo's presentation focussed on the importance of social media platforms as a key medium to disseminate propaganda during times of conflict. She discussed the results of two studies involving content analysis of visuals used for propaganda purposes.

Describing the nature of a network information society, which many societies around the world had become, she underlined three characteristics that were important: (a) there was a significant reduction on the dependence on mass media; (b) non-market production or non-profit collaboration between individuals to produce online content was growing; and (c) the decentralisation and democratisation of information was becoming apparent.

She then went on to discuss the differences between online text and visual elements, and argued that images were more likely to grab attention and generate interaction. This was observable in the photo albums on Facebook pages that generated greater levels of engagement. This ability to grab attention helps to explain why visuals on social media websites are actively used in messaging for propaganda and/or persuasion.

To illustrate her point, she referred to the targeted killing of Ahmed Jabari, senior leader of the Izz ad-Din al-Qassam Brigades, the military wing of Hamas, by the Israel Defense Forces (IDF) in November 2012. Following the announcement of his death on Twitter, exchanges between the IDF and al-Qassam brigades intensified. Seo explained that 'resistance' was a prominent theme of the IDF online posts, followed by 'unity' and 'threats from the enemy'. By contrast, Twitter images posted by the al-Qassam brigades first emphasised 'casualties of civilians', then 'resistance' and then 'unity'.³

Two major thematic areas were subsequently compared: one involving the sense of unity and self-sacrifice of Israeli soldiers on one hand and the sufferings of Palestinian civilians on the other. In terms of categories and

³ "The 'resistance' category covered images that convey defeating the other side or getting prepared for combating the other side – for example, Israeli soldiers attending training sessions and Hamas images of its M-75 projectiles. The 'threats from the enemy' category covered images showing military capabilities of the other side such as missile launch sites or leaders of the other side drumming up support for military attacks. The 'casualties of own civilians' category covered images of death, injuries, and suffering of innocent civilians of their own side. The 'destruction' category covered images of buildings in their own territories being destroyed by attacks from the other side. The 'unity' category covered images aimed at promoting solidarity among their own military personnel or civilians. Examples of images conveying the theme of 'unity' include Hamas posters asking people to show solidarity with Palestine prisoners jailed in Israel who were on hunger strikes and photos of a massive rally in Gaza celebrating the 25th anniversary of Hamas. The 'humanity' category covered images emphasising their efforts to protect civilians of the other side". See Hyunjin Seo, 'Visual Propaganda in the Age of Social Media: An Empirical Analysis of Twitter Images During 2012 Israeli-Hamas Conflict', Visual Communication Quarterly, Volume 21, Issue 3, 2014, p. 153.

frames⁴ employed, Seo observed that there were 'analytical' and 'emotional' categories, 'overt' and 'covert' frames, and 'human interest' and 'non-human interest' frames. A typical example of a message conveyed under the 'emotional' category was a picture of Palestinian parents crying beside the dead remains of their child/children.

The second study involved the analysis of several hundred Facebook images posted by supporters of the Syrian government and the Syrian National Coalition (SNC). The theme of unity featured prominently in visuals related to the Assad regime, both to emphasise a semblance of normality and to mobilise support. On the contrary, civilian victimisation seemed to be a key component of the SNC's Facebook communication strategy. The contrast between the overt propaganda frame, widely used on images posted by the SNC, and the subtlety of the Syrian government's propaganda message was underlined.

Assessing the impact of these visuals on the audience, Seo mentioned that images featuring human interest were effective in eliciting reaction from the public: audience reaction is likely to be triggered by the ways certain themes are addressed, such as the disastrous consequences of the conflict on the education of children of a given Syrian family. In closing, she mentioned that real-time engagement has increasingly become an essential element of online propaganda, as shown by the effective work of the IDF in this area.

Discussion

A participant wanted to know if a deeper understanding of politics was a prerequisite for an individual to effectively determine information from misinformation. A speaker replied that while this was true, it was still difficult to change perceptions when they were already embedded within a society. He argued that some individuals would simply not believe the corrected information.

A participant enquired as to how to develop effective counter-arguments especially if these go against an individual's world view. A speaker explained that one of the ways to mitigate this is by framing the message in a way that reduces the threat to self. A speaker from another panel added that it could also be done through less aggressive means of arguing, such as interactive deliberation rather than one-way messaging. Also, decontextualising information such as taking away partisan cues to make it seem more neutral was also useful.

A participant enquired as to how public trust between law enforcement agencies and the general public could be increased. A speaker replied that the authorities have to manage society's expectations to gain confidence and trust but this could only occur over time. Public officials have to be careful with the claims that they make as well as how the messages are composed and delivered. For example, the NSWPF has successfully gained public confidence by producing television programmes about their work and the cases they have solved, as well as using social media platforms to showcase their work so as to be more relatable and relevant to the people. There is also a customer service focus and an educational purpose in all outreach activities.

A question was raised as to how to discern if reports/ stories posted on an organisation's social media platform were real. A speaker replied that the NSWPF has a 24-hour media unit that serves as the first point of information processing with staff trained to determine the veracity of these reports. Moreover, the NSWPF has media-related standard operating procedures (SOPs) that serve as an overarching guide. The problem,

⁴ "The 'overt propaganda' frame covered images that explicitly blame the other side for the renew violence and killing innocent victims. The 'covert propaganda' frame covered images that implicitly label the other side as an "evil". The 'analytical propaganda' frame covered images that provided facts about how the other side destroyed them, how they are prepared to defeat the other side, and what the public should be ready to do. The 'emotional propaganda' frame covered images that aimed at raising awareness or attract attention by eliciting emotions such as anger against the other side or sympathy toward their own people. The 'human interest' frame covered images that highlight stories of individuals who suffer from attacks from the other side making the viewers feel that the stories are personally relevant to them and feel emotionally connected to those individuals and thus to the message. Human interest frames have been widely used in textual and visual propaganda as they tend to elicit strong emotional reactions". See Hyunjin Seo, 'Visual Propaganda in the Age of Social Media: An Empirical Analysis of Twitter Images During 2012 Israeli-Hamas Conflict', Visual Communication Quarterly, Volume 21, Issue 3, 2014, pp. 153 – 154.

however, is not so much about information processing but rather how to respond as humanly and efficiently as possible. The NSWPF have learned that citizens prefer responses that are tailored, humorous and show a personal touch as opposed to impersonal and machine-generated type messages.

Another participant asked about the coordination efforts between the different bureaus and law enforcement agencies, as well as between the media and law enforcement agencies in New South Wales. A speaker replied that relationships between the various stakeholders and the NSWPF are good, and have been carefully built up over time. There were many operational advantages for maintaining collaborative relationships between stakeholders.

A participant enquired about the role of narrative frames in both textual and imagery information. A speaker pointed out that although much research has been done on narrative framing and its influence on people's thoughts and reactions to an issue, one has to be mindful that framing is not always done consciously. The framers do not necessarily have the intention or the motivation to frame things in a certain way. Based on the speaker's research on a group of journalists, it was found that there is often a gap in what communicator's try to say and how their audience understands it. Such limitations should be taken into account when conducting research on media and framing.

Another participant enquired about the role of authorities in influencing/shaping perceptions. A speaker replied that while the authorities can indeed be influential in shaping perceptions, they must be sensitive to the needs of the audience. It was suggested that when addressing any posts on social media that generate negative feedback, a strategic approach was useful. Also, humour, apologising and acting with humility at the appropriate juncture were good ways to de-escalate conflict.

PANEL 4:

TOOLS FOR SOCIAL MEDIA ANALYSIS

Social Media Science: Implications for Research, Analysis and Policymaking

Carl Miller, Research Director, Centre for the Analysis of Social Media (CASM), DEMOS, UK



Carl Miller

In his presentation, **Carl Miller** spoke about how researchers can study beliefs and attitudes from social media analytics. Through a number of case studies, he talked about the new technologies and methods that were needed to carry out social media research more effectively. He also highlighted new risks and dangers inherent in the social media research: how far this new form of research can be trusted, when it can be used, the value such use could bring, and how its use can be made more publicly acceptable and ethical.

Miller highlighted that social media users currently comprise more than a billion people worldwide. The rise of social media platforms has created unprecedented quantities of data about society and made the study of human behaviour and society possible. He also noted that social media data is voluminous, rich in links, and unmediated. It constantly refreshes in real time. While in the past, it had been impossible to listen to millions of voices in real-time, now researchers can understand events as they are taking place because the Internet serves as a repository of online activities. Therefore the lapse between the actual event and analysis is greatly reduced. Thus two parallel revolutions had taken place: the explosion of data and the ability to

understand it better. Social media intelligence is the outcome of such revolutions.

Miller saw turning this data into social insights as one of the most important research challenges for this generation. If successful, it could lead to transformative steps moving forward in terms of analysing how society works - its dynamics, processes, tipping points and mechanics. This could, in turn, lead to more informed, more agile and more data-rich decision-making and policy-making.

He highlighted some ways in which social media has been used to understand events. For example, by studying the volume and measuring change in the rate of tweets relating to the 2012 Olympics over time, Miller observed that every medal won was literally a social event as it was characterised by the sudden increase in volume of tweets relating to that specific sporting event.

Social media research had also studied unexpected events such as the London riots of 2011. In unexpected events, no online activity provides any indication of the events prior to its outbreak. However, it is possible to study other trends after the outbreak of these unexpected events such as social networks. In addition, it is now possible to study sentiment in real-time on the social media.

In conclusion, Miller highlighted that social media research currently has little implication for policymakers due to its inability to satisfy basic evidentiary requirements for policy makers. He argued that social media research needed to step beyond analytics as well as to become a new intellectual discipline in order to tap its full potential.

TALISON - Tensor Analysis of Social Media Data

Anne Kao, Senior Technical Fellow, Boeing Research and Technology



Anne Kao

In her presentation, **Anne Kao** observed that with the growth in social media, online forums have become major sources of data for social network analysis and a major research area in data analytics. However, many aspects of social networks have not been addressed fully, if at all. The TALISON (Tensor Analysis of Latent Interactions in Social Online Networks) software is able to fill in this gap through the analyses of Twitter data using tensors that are able to capture various parts of the content of online exchanges, take into account the different forms of relationships and track the temporal dynamics and evolution of topics on the social media.

Kao noted that the wealth of open source data is a potential source of value for both private companies as well as the government. However, open source data represents several challenges for data mining: (a) huge volume; (b) diverse and complex format; (c) complicated nature of internet data collection or crawling processes; and (d) difficulties faced in data preparation and cleaning.

She highlighted several aspects of social network analysis that require attention. First, there is the need to capture various parts of the content of the exchanges, for example, bare text and hashtags, which constitute some of the major features of social media networks. Second, as in all social networks, there are many different types of relationships, for example, "following" and "friend" relationships, as well as relationships defined in terms of how users interact with one another

such as replying, quoting, retweeting, and mentioning. Finally, an important aspect of analysing social networks is temporal dynamics and topic evolution. Kao offered an analysis of Twitter data using tensors which can incorporate all of these different aspects in a single representation and identify both salient events and distinguish important views of these events.

Kao observed that most social media analysis also tends to be weak in analysing text. Existing software uses quoted string only and examines highly limited content, while simple content analysis tools are only able to process tens or hundreds of millions of content. Without better text analysis, results are often not detailed enough and therefore not 'actionable'. Furthermore the learning curve for text analysis is extremely steep.

The tensor model of social media analysis promises to address the above weaknesses in social media analysis. A tensor is a multidimensional array of data that can be conceptualised as an extension of vectors and matrices to higher dimensions. Tensors are used to represent multiple relationships, among documents (such as tweets), authors (such as authors of tweets and retweets), terms (which can also include hashtag as a special category), time, and space.

Applying tensor analysis to social media allows many advantages such as: (a) modelling and synthesising multiple types of relationship simultaneously; (b) revealing topics and relationships simultaneously; (c) revealing changes in topic over time; and (d) allowing results to serve as a summary that is easily understandable by analysts.

Kao concluded by observing that as technology improves, that social media analysis will be able to incorporate sentiments, opinions, and location information. Expedited analysis of large quantities of data will also be possible.

EMBERS: Forecasting Civil Unrest using Open Source Indicators

Brian Goode, Postdoctoral Research Associate, EMBERS Project, Discovery Analytics Center, Virginia Tech



Brian Goode

Brian Goode presented on the technological aspects of EMBERS (Early Model Based Event Recognition using Surrogates), a fully automated 24x7 continuous system for forecasting population-level events such as disease outbreaks, civil unrest, and election outcomes using data from open source indicators. Created by the Discovery Analytics Center (DAC) at Virginia Tech, EMBERS has been making forecasts into the future since November 2012. EMBERS had been successful in forecasting the June 2013 "Brazilian Spring", the February 2014 violent student-led protests in Venezuela, and the recent protests in Mexico that related to the mass kidnappings of student teachers. Goode's presentation described the architecture of the EMBERS system, event forecasting methods, performance metrics, and the methods by which forecast data is communicated to end-users.

The EMBERS Project is funded by the IARPA Open Source Indicators (OSI) program. It aims to develop methods for continuous, automated analysis of publicly available data in order to anticipate population-level events such as protests, riots, elections, disease outbreaks, economic instability, resource shortages, and responses to natural disasters. The OSI program focuses on the regions of Latin America and the Middle East. Some events that had been successfully forecast by the EMBERS system included the riots after impeachment of the Paraguay president, the "Brazilian Spring" of June 2013, Hantavirus outbreaks in Argentina and Chile, the Venezuelan student uprising of February 2014 and the 2014 elections in Panama and Colombia.

Goode explained that the predictive analysis of the EMBERS system employs novel surrogates for specific event classes. It also integrates model-based and data-driven methods by combining causal and statistical approaches to epidemiological forecasts. It possesses a comprehensive suite of forecasting algorithms aimed at capturing different classes of spatial and spatiotemporal compartmentalisation patterns.

Goode discussed several key strategies used by the EMBERS system for forecasting civil unrest. Firstly, it examined a multitude of data sources such as news, tweets, blogs, TOR (a

free software that protects an individual's identity on the internet), Integrated Conflict Early Warning System (ICEWS), Global Data on Events, Location and Tone (GDELT), Currency, LADB, smiles.

It also utilises a multitude of models such as planned protest, spatial scan, cascade regression, dynamic query expansion, volume-based LASSO model and baseline model. The models are fused together for analysis in order to see which model is best suited for analysing a particular event. In addition the system is able to retrieve suitable quality data to enable accurate forecasting.

According to Goode, multiple trade-offs exist in the EMBERS system, including precision-recall, recall-quality and quality-lead time. The researchers are committed to supporting single dial functionality for each of these trade-offs and interaction exploration across these trade-off boundaries according to user preferences. He also showed the user visualisation tools of the system, which is able to provide word or map of time of occurrence of the events. The audit trail interface of the system was also shown. Goode concluded by summarising the key features of EMBERS and how it has been used in predictive analysis.

Discussion

A participant wanted to know if using sentiment analysis was sufficient in analysing social media data. A speaker replied that sentiment analysis obscures more than it illuminates. The numbers churned out hide the fact that often the researchers are unsure what they are in fact counting, what social reality they are actually

tapping into, and how accurately they are actually doing that. Therefore there is the need to move beyond this. Sentiment analysis is currently able to just look at positive and negative tweets.

A participant wanted to know about the changing roles of the mainstream media and social media, and in particular, how and if mainstream media provides a multiplication effect for social media. A speaker replied that while social media was certainly changing the way mainstream media operated, it was not eclipsing it. Social media should be seen as contributing to mainstream media; adding to the mix, but not completely separated from it.

A participant enquired as to whether developments in link analysis could help determine influencers or how to change sentiments. A speaker replied that while there had been improvement in the technological side of the house, people were nowhere closer to understanding what they were studying and how different things were from the offline world. There was a need to qualitatively study different scenarios whilst embracing technological advancements.

A participant wanted to know how to analyse sarcastic tweets since tweets were purely text and did not show facial expressions or normal features of speech such as intonation and pauses. A speaker replied that accurately interpreting meaning from data extracted from tweets and Facebook posts was an ongoing challenge since almost all data collected is usually contextual and aggregated. Moreover, as the participant had pointed out, the absence of non-verbal cues makes the task even more challenging. Notwithstanding, sarcasm was actually an area where analytical improvements have been made. The use of sarcasm is linguistically quite distinctive; it is quite different from non-sarcastic use of language. More sophisticated models are being developed to help with determining sarcasm and attempting to understand the real meaning behind the tweet(s). There is movement from naïve approaches such as basically just looking at bags of words to distributional semantics.

A participant highlighted that there were legal and practical difficulties that could arise if incorrectly deriving meaning from tweets. An example from the UK was cited. A speaker replied that the issue highlighted

the failings of the criminal justice system and legal process, and not about the inability to accurately determine the true meaning from the tweets.

A participant enquired as to whether social scientists could use tensor analysis of social media data (TALISON). A speaker responded that there was actually a big move in the US to combine social science with social network analysis. The goal was to determine if social theories could adequately explain computer data. But as this idea was still very new, and not much has been done to identify the relevant social theories, developments have not been forthcoming.

A participant enquired as to how Tensor enhances sentiment analysis. A speaker replied that most software works by pre-selected keywords, but people do not necessary talk that way online. TALISON does not pre-select terms because we do not know what words people use. It also does not pre-select hashtags. It uses a data-driven approach which uses seed words, which is then followed by correlation.

Another participant wanted to know how advanced sentiment analysis was for multimedia. A speaker replied that generally two different approaches were used. The first was a dictionary based approach. The problem with this approach is that it is difficult to perform analysis in multi-languages, and the data may not contain enough terms for analysis. The other approach is the statistical approach, which involves allocating some seed terms and see how one's data is related to the seed term. However, when using this approach, one has to be careful with the context as people use different terminology, depending on age and cultural backgrounds.

A participant wanted to know if there was a number EMBERS used for critical mass and tipping points for events. A speaker replied that EMBERS analyses tweet cascades, which is, in turn, able to build an information cascade beginning with a single user. There are different libraries of curves in terms of information spread. With a certain percentage of users it can determine if the critical mass was built. The EMBERS team is currently doing a retrospective study of Brazilian and Venezuelan elections to evaluate this. The cascade model is highly dependent on factors such as highly influential people as well as particular behaviours and trends.

A participant wanted to know if EMBERS could forecast happy/pleasant events. A speaker replied that EMBERS does not forecast happy events per se but focussed mainly on civil unrest or protests. The speaker also clarified that while a lot of images and language used may give the impression that all civil unrests are negative, in some countries, civil unrests are legal. When conducting research on these events, EMBERS researchers focus purely on the dynamics, and do not make value judgements of whether the event was 'good' or 'bad'.

Another participant wanted to know if EMBERS used their predictive capabilities proactively. A speaker

replied that the software stops at the analysis level. It was not used for any active inference. For example, if an Ebola outbreak is predicted, the data would be published on the website, and the funding agency decides what to do with it. Their role is to produce the forecast as an academic exercise.

A participant wanted to know if incorrect predictions occurred and how they were handled. A speaker replied that incorrect predictions did occur, and that was part of the quality score. At the end of the day the tools are all probability models, and as such, not a hundred percent accurate. Hence, researchers are mindful of the sensitivities that relate to inaccurate predictions.

PANEL 5:

LEGAL AND REGULATORY FRAMEWORKS

The Problem of Regulating Open Source Intelligence Gathering in the United Kingdom

Simon McKay, Principal, McKay Law Solicitors and Advocates



Simon McKay

Simon McKay discussed the emerging problem of open source intelligence gathering in the United Kingdom (UK), where there is no clear legislation that would provide authorisation to government agencies to gather data or acquire information on social media or the Internet. McKay highlighted that there is also ambiguity in the legal roles of the courts and the oversight bodies, as well as convolution between the laws already in place regarding the rights of an individual to privacy.

McKay first explained the problems that currently exist in the UK. There is a complex legislative structure that permits the authorities to take action, but at the same time quasi-judicial opinions can be expressed that ultimately interfere with this process. For instance, the Security Service Act (1989), Intelligence Service Act (1994) and Police Act (1997) provide the legal basis for agencies to acquire and discharge covert information. While the Regulation of Investigatory Powers Act (RIPA, 2000) regulates how agencies carry out surveillance, investigation and interception of communications. In addition, the Data Retention and Investigatory Powers Act (DRIPA, 2014) regulates how intercepted data is handled and retained. The conundrum arises as English Law also recognises the right to respect individual

privacy, which is fundamentally at odds with the laws that allow the covert acquisition of information. Critics have also maintained that such laws directly affect an individual's right to freedom of expression.

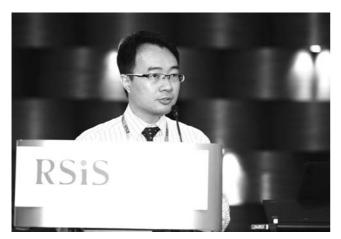
McKay elaborated on the legal challenges that pertain to this issue. He questioned the adequacy of existing laws and Strasbourg jurisprudence as these could have widespread implications for national security and policing. The tensions between fulfilling domestic needs for national security with privacy and other rights as well as the right to a fair trial would only worsen if these issues were not sorted out. McKay opined that there might be risks of 'rights drift' (or the non-satisfaction of one's individual rights when the law takes importance). Furthermore, the existing legal issues might result in breaches of authorisation: for example, the existence of RIPA and DRIPA as regulatory frameworks did not mean that the procedures of how covert information was gathered could not be challenged.

McKay also discussed some operational challenges for security agencies if the laws remained unclear and confusing. The biggest challenge would be in terms of undermining public confidence in the security, policing and law enforcement agencies in the UK as many have and would question how such agencies are managed. Operations would expectedly be adversely affected as well. Rather than developing new legislation, McKay opined that sharpening the quality of existing laws would be more useful. This included addressing issues such as 'rights drift' and the impact of decisions made under Strasbourg jurisprudence.

McKay concluded by providing offering insights on how best to address these challenges. He suggested that legislation should be simplified, and that there should be a clarification of the constitutional rights of the citizenry. A review of the laws' ultimate objectives and an assessment of the methods used in covert policing should also be carried out. At the same time, the government should increase transparency and accountability.

Study, Search and Seizure in Social Media – The Legal and Regulatory Framework in Singapore

Benjamin Ang, Education Chair, Internet Sociey (Singapore Chapter) and Lecturer, School of Business, Temasek Polytechnic



Benjamin Ang

Benjamin Ang discussed the legal and regulatory framework in Singapore that pertained to the use of data attained from private/public domains as well as from social media platforms for the purposes of investigation, research and analysis. These included: (a) Computer Misuse and Cyber Security Act; (b) Personal Data Protection Act; and (c) Criminal Procedure Code of Singapore. He also discussed the powers granted to key stakeholders and the authorities, scenarios under which these powers would have effect, and the penalties for the unauthorised use of social media data.

The Computer Misuse and Cyber Security Act is the main legislation governing all major activities in cyberspace. The law prohibits unauthorised access to a computer; attainment of data or programme(s) held in any computer is only lawful with the permission of the device's owner. The law also prohibits the unauthorised disclosure or sale of access codes (for example passwords, tokens). Penalties for breaches include fines or imprisonment. However, these prohibitions do not apply to investigations conducted by law enforcement officers and authorised personnel. Furthermore, in the event of a national security threat, law enforcement officers and authorised personnel have the power to compel individuals to access a computer and provide any information that would help counter the threat even if such information is privileged and proprietary.

The Personal Data Protection Act governs the collection, utilisation and release of personal data in both electronic and non-electronic forms – from which the identity of the said person can be distinguished. This protects the individual from the misuse of their personal data, especially when it is being passed on to a third party or organisation.

The second schedule delineates that it is lawful for an organisation to collect the data without consent if it is for the purpose of the national interest and/or any investigation or proceedings (if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data). The third schedule dictates that the use of personal data without consent would be lawful if it is for the purpose of the national interest and/or any investigation or proceedings. The fourth schedule allows an organisation to disclose personal data about an individual without consent of the individual if it is for the national interest and/or any investigation or proceedings and/or to a public agency and such disclosure is necessary in the public interest.

Section 39 of the Criminal Procedure Code of Singapore 'Power to Access Computer' grants a police officer or authorised personnel, who is investigating a criminal offence, the power to access a computer or gain access to a computer without consent if he/she has reasonable cause to suspect that the computer is or has been used in connection with the criminal offence. Any individual who attempts to obstruct the police officer or authorised personnel may be fined or imprisoned or both.

In sum, Ang noted that there were sufficient laws in Singapore to regulate the use, collection and data on and offline, identification of who could legally have access to such data and the penalties for breaches. This was extremely important since today there are more transactions and activities that require one to volunteer one's personal data especially in cyberspace.

Developing a Regulatory Framework for Social Media Analysis and Investigation: Key Components and Issues

Simon Chesterman, Dean, Faculty of Law, National University of Singapore



Simon Chesterman

Professor Simon Chesterman argued that contextual changes within a society were fundamental in thinking about approaches on how to deal with the regulation of social media for analysis and investigation. He highlighted three areas that were important in this regard: (a) changing nature of threats; (b) changing technology; and (c) changing culture.

In relation to changing threats, a society could experience a major change in how it defined threats as well as where the threat threshold was (i.e. before government intervention is deemed necessary). For instance, global understandings of 'intelligence' and 'national security threats' have significantly changed over the last decades. For example, countries supporting capitalism, and by extension, the US and its allies, were once regarded as enemies of countries supporting communism and the Soviet Union and vice-versa. With the end of the Cold War, new threats have since emerged, such as terrorism, and have compelled a re-definition of national security threats and security priorities.

With regard to changing technology, laws will always lag behind technological advancements, since it is impossible to accurately determine how these advancements will be used (i.e. for good or evil). Greater attention should be paid to the online sphere as more people are consenting to the use of their personal data on online platforms, which in some

cases, is routinely shared. Of concern is whether power would actually move into the private sector since it is private companies who are collecting the bulk of the data and not government. This would expectedly make access to such data more difficult.

As for changing culture, one's understanding of privacy has changed dramatically as well, and to some extent, it has become paradoxical. For example, some people are anxious that governments have access to their personal data through identification cards or tax file numbers, and now with the integration of governmental functions. However, they volunteer their personal data when shopping online or when using social media applications, despite the fact that this is not always secure. For example, there have been cases where individuals unknowingly or knowingly divulge personal information about their family/friends/associates to unauthorised third parties. There has arguably been a paradigm shift from concerns about how personal data is collected to how it is being used.

In conclusion, Chesterman argued that the evolving socio-political context in Singapore would necessitate a deeper understanding of how social media is used as well as the changing expectations of society, in order to better develop a framework for social media analysis and investigation.

Discussion

One of the participants asked about the debate around CCTV and infringement of privacy in the UK context. It was affirmed that there were tensions related to the use of CCTV in the UK. On one hand, CCTV is very widespread that there is a general acceptance that some infringement of privacy occurs in public places. On the other hand, the Regulation of Investigatory Powers Act (RIPA) stipulates that the use of CCTVcaptured images for criminal investigation requires authorisation. The irony of RIPA is that it restricts law enforcement's authority to keep surveillance on potential criminals but not on the general public. In some cases, the problem is not in the acquisition of CCTV footage per se but rather in its use. For instance in the Geoffrey Peck case in which the local government publicised the CCTV images of his suicide attempt, the court decided that his privacy had been violated

because the press had used a mix of unclassified CCTV footage with other personal information obtained from classified sources.

Another question that was raised was whether the UK had similar laws like Singapore that enabled authorities to carry out investigations online. A speaker replied that the UK did not have such legislation. Nevertheless, there is still uncertainty and debate on how 'covert but overt' information can be used in online investigations, and on how RIPA and DRIPA might be used in this regard. It was suggested that since there is a fundamental difference between obtaining information as a private individual versus obtaining it for the state, a clarification must be made at the outset on why the data was being collected, that is, whether it was for personal purposes or for national security purposes. RIPA and DRIPA were not intended as laws to deal with crime, but laws to protect privacy.

A participant enquired as to what the main implications were with regard to laws regulating privacy on social media. It was suggested that the authorities should spell out explicitly what the information collected would be used for, and how it would address instances whereby information was attained secretly. For example, when an individual has information on future events that may jeopardise national security but obtained covertly, how does he or she report it? Another example is who would be responsible for the occurrence of an event (e.g. a riot), if action was not taken despite having the intelligence. These were possible issues that needed to be thought through carefully.

A question was raised on whether Singapore's data protection laws were adequate. Some gaps in Singapore data protection act were discussed. The flexibility of the data protection act could be a source of weakness and strength. The weakness is that it contains multiple vague terms that might create confusion when attempting to implement practically. At the same time, some degree of flexibility enables government agencies to do their job. However, it was noted that what might appear as flaws in legislation actually reflects the kinds of purpose it serves. For example, the EU approach to data protection might seem restrictive because it was driven by human rights concerns and aimed at limiting the government's power over the citizens. Meanwhile the US data protection legislation

might seem too liberal to some because it was aimed to protect the interests of the business sector in addition to individual rights. Likewise, the Singapore data protection act may be flexible by design in order to enable operational activities.

A participant asked if the privacy laws in Singapore could be used in cases where an individual was harassed online (social media) and then subsequently harassed in real life by the actions of his/her online tormentor. A speaker replied that this was possible as social media was used to mobilise action against the individual, which could be considered 'public incitement'. Additionally, Singapore has the Cyber Harassment Act, which would protect individuals from online harassment and cyber-bullying, as well as stalking. This act, together with the Computer Misuse and Cyber Security Act, would be the main legislation used when investigating such a case.

A participant asked how a person could determine whether information they put on social media was likely to be interpreted as a potential threat to the national interest. In light of possible 'grey areas', should the public be made aware of what the boundaries were, and if so, would public education help. A speaker replied that there have been cases where the line was clear, and the originator of the post clearly crossed the line (e.g. 'I'm going to blow up the Parliament!'). Through investigations, the true intentions of the composer of the post will be made clear.

A participant enquired about the 'right to be forgotten' principle on social media. A speaker replied that the 'right to be forgotten' principle is a European initiative that might be inapplicable to Singapore. What individuals should be cognisant of is that 'data protection' today should be about managing how data is being used instead of removing it fully, as this might be difficult. With the Personal Data Protection Act, the onus is on the individual to withdraw his/her consent of how their data is being used. This is can be challenging especially if the third party has sold the data to another party.

A question was asked on changing technologies and the role of private companies, and if there was a need to balance national security concerns with commercial interests and the respect for privacy. A speaker replied that this was an existing paradox, where ironically, most people would fear a person whose job was to spy on their Facebook profiles as opposed to a whole infrastructure automatically devoted to the surveillance of their communication and operated by a private company. The emphasis therefore was on how the gathered information would be used.

A participant wanted to know if the threat to privacy was a significant consideration given that so much data was collected, transmitted and stored online. A speaker replied that this was a trade-off: the benefits/convenience of having one's personal information data collected and available in return for sacrificing a little privacy.

PANEL 6:

CASE STUDIES 2

Using Social Media Analysis for Emergency Preparedness

Rafael Lemaitre, Director, Public Affairs, Federal Emergency Management Agency (FEMA)



Rafael Lemaitre

Rafael Lemaitre presented on how the Federal Emergency Management Agency (FEMA) manages emergency communications as the main agency for emergency preparedness in the US. FEMA's responsibilities include: helping communities and individuals know what they need to do in the event a disaster occurs, and to this end, social media platforms have proven to be useful in informing and educating them about emergency preparedness.

Lemaitre discussed National Preparedness Month, an integrated national campaign conducted every September, which aims to communicate the importance of being prepared, as a case study. In 2014, FEMA decided to focus on encouraging Americans to build a family communications plan. The message emphasised the need for families to come up with their own strategy in case members are separated from each other and mobile communication devices are unusable. To ensure that this message made an impact, FEMA released a powerful and emotional public service announcement via social media channels. The announcement portrayed two families, one with members together in a disaster shelter and another with only a pair of parents arguing, crying, and trying to figure out where their children are.

Aside from posting the announcement on various social media platforms, FEMA also used Thunderclap, a tool which allows a message to be mass-shared by recruiting people to post it at the same time. By using Thunderclap, FEMA is using a sort of 'word of mouth marketing' as one can see their friends sharing the same message two or three times in his/her newsfeed. As the message originates from friends, one is more likely to pay attention. According to Lemaitre, FEMA had great success in using this strategy and the organisation was able to reach 6.7 million people with the message of getting involved in the National Preparedness Month.

To ensure that the dissemination of information is successfully maintained, FEMA put together different metrics to analyse the level of impact of its online posts. FEMA's analysis tools include recording the number of visits to its websites, ranking its Facebook posts according to popularity, evaluating the best time to post digital content, assessing whether graphics and hash tags were used in the most popular posts, and using word clouds to determine how many times a word has been mentioned in social media conversations.

Lemaitre concluded his presentation with some recommendations on how to effectively disseminate information through social media: (1) 'fish where the fish are'; (2) leadership is key; and (3) 'be human'. The first suggestion touches on the importance of posting content where the audience actually are rather than where you think they are. FEMA is aware that more people visit online news websites such as The Huffington Post than FEMA's official websites or blog, therefore it posts blog entries on the popular news site as well. The second recommendation focuses on the importance of leadership. Lemaitre highlighted that FEMA's administrator Craig Fugate does not only support the use of social media in FEMA's campaigns and announcements but he also uses it himself. Lastly, to be human means to engage with your audience. Replying to comments, tweeting back, and connecting with netizens do go a long way.

Application of Open Source Intelligence (OSINT) for Crisis Management: An Overview of the ATHENA Project

Babak Akhgar, Professor and Director of CENTRIC, Sheffield Hallam University



Babak Akhgar

The Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research (CENTRIC) uses open source intelligence (OSINT) for national security and crises. To elaborate on the different aspects of OSINT, **Babak Akhgar** used CENTRIC's ATHENA Project as a case study. The ATHENA Project aims to use social media to develop the ability of citizens and first responders in dealing with crisis situations.

Akhgar explained that OSINT is a form of intelligence that is publicly available and accessible through various sources including social media. Nowadays, information can be gathered from content generated by social media users, and is also free. However, as convenient as it may sound, OSINT can also pose some challenges. As OSINT heavily relies on what people post online, the accuracy and credibility of some of the information they provide could be questionable. After the Snowden revelations, people have become more conscious about the material they post online, and thus some of them even use false names, occupation, date of birth, and other details. Akhgar argued that this has a direct significant effect on the quality of OSINT. Therefore, to ensure that OSINT is used effectively, it should be combined with traditional information source and heavy analytical processing.

One of the programmes created to ensure that OSINT is applied to crises effectively is the ATHENA Project. A result of high-level discussions and the cooperation of

various entities, ATHENA aims to provide the following: smart mobile devices which can be distributed to the members of the public and first responders, command and control capability, analytical processing of social media (which includes natural language processing capability), proactive monitoring of social media, and reactive decision-making capability. ATHENA is also able to deliver live sentiment analysis of the police, first responders, public events, and specific incidents. Compared with reactive sentiment analysis, live sentiment analysis can help with decision making during a crisis.

The ATHENA platform recognises that the members of the public are the best reporters especially since social media use is rampant these days. Akhgar pointed out that the members of the public are usually the first ones present in the scene of a disaster or crisis. With the images and videos that people post, ATHENA can monitor real-time social media feeds from anywhere in the world. As long as the posts are publicly available, ATHENA can access and process them. However, as mentioned previously, guaranteeing accuracy is a challenge in the age of social media. Akhgar explained that a huge number of rumours and misinformation could be posted as well, and thus it is important to quickly discredit these and provide an alternative view via ATHENA's language processing and explaining capabilities. In addition, it is always useful to compile data to create a holistic process.

Social Media and Mobile Forensics

Christopher Church, Digital Forensic Specialist Digital Forensic Lab, INTERPOL Global Complex for Innovation, Singapore



Christopher Church

Representing the International Criminal Police Organization (INTERPOL), **Christopher Church** talked about how social media and mobile forensics was used to solve crimes and handle crises. He explained that a large number of social media users access their accounts or pages via mobile devices. In addition, millions of people use instant and social messaging apps such as BlackBerry Messenger (BBM), ChatOn, Facebook messenger, iMessage, Line, Skype, Tango, Viber, WeChat, and WhatsApp. All of these platforms can play a crucial role in conducting criminal activities.

Church argued that while open-source data is useful, criminals sometimes opt to use alternative instant messaging services to avoid detection by the police. For instance, instead of using Twitter, gangs behind the London riots used BBM to broadcast to their members where the police were, and as a result, were able to move to a different location to evade the authorities. It is easier to transmit information, provide updates, instructions and plans, while also excluding unwanted receivers or audiences on mobile messaging apps.

Aside from riots, another type of crime that could be carried out using the above-mentioned apps is 'sextortion'. Sextortion is done via video chats, where the offender convinces an individual to remove his or her clothes in front of the web camera. The individual is recorded, and as such, is highly vulnerable. Sextortion victims are asked to pay a certain amount of money, and refusal would result in threats to release the video recording of the victim on social media channels. According to Church, INTERPOL has worked on such cases in several areas in the Philippines, Hong Kong, Australia, United States, and the United Kingdom.

Two of the most challenging offences brought about by social media and/or social networks are trolling and harassment. Trolling is obviously pervasive in the age of social media, nevertheless, there is still a huge gap between the offence and how law enforcement responds. Ironically, sometimes criminals or wanted individuals taunt the police on social media but in doing so, reveal clues about their location, and are summarily apprehended as a result. Harassment can come from the use of dating apps. However, when authorities analyse the messages of the individuals involved, sometimes, the complainant appears to have facilitated the harassment.

In closing, Church observed that people rely heavily on smartphones for purposes other than communication and applications such as controlling and accessing devices in homes, offices, and public spaces. This technological advancement could enable crimes and incidences such as hacking, spying, robbery, and transmission of indecent images.

Discussion

A participant enquired as to how FEMA maintained a list of verified Twitter accounts during civil emergencies, and how these accounts were selected. A speaker replied that as the US operates on a federal system, the federal government has certain powers. Major disasters are handled by the local authorities of the 50 states that make up the USA. Only when the crisis exceeds the ability of states to respond and recover, FEMA is mobilised. When we see something like the snowstorm in New York occurring, we are able to see who in the state emergency management can deliver relevant help. These are always handled by government agencies or elected officials, not any lay person. So these Twitter accounts belong primarily to these local government agencies.

A participant wanted to know how Thunderclap actually worked. A speaker replied that Thunderclap is a free and open system whereby a user can log in and write his or her own message and start their own social campaign. The campaign will invite receivers to sign up for Thunderclap or email a list of people to advertise the campaign to. Once a particular campaign reaches 250 supporters, Thunderclap will push that to all networks that have signed up for it. It is a very suitable system for advocacy and political campaigns based in the US but anyone can use it.

A participant wanted to know how FEMA uses social media to raise awareness during disaster recovery. A speaker replied that as an example, FEMA did a lot of work in terms of providing shelter during disasters. While FEMA itself does not provide shelter facilities, its app re-tweets requests for shelter as well as helps people look for shelter during recovery. Furthermore, the FEMA App contains preparedness information for different types of disasters, an interactive checklist for emergency kits, a section to plan emergency meeting

locations, information on how to stay safe and recover after a disaster, a map with FEMA Disaster Recovery Center locations (one-stop centers where disaster survivors can access key relief services) and Shelters, general ways the public can get involved before and after a disaster, and the FEMA blog.

A participant wanted to know if FEMA would be using social media to crowd source in future. A speaker replied that Hurricane Sandy was the first crisis in which FEMA had to determine how to develop effective messaging and how to use social media more effectively during a major disaster. One of the things that FEMA did was to set up a rumour control page. This was envisaged to find out what people were saying online especially if these were rumours. In fact there were many rumours like FEMA was running out of water, certain bridges were inaccessible but in fact were. After Hurricane Sandy, FEMA began to realise the value of social listening, hence the digital team was expanded and a section focusses specifically on digital engagement and social listening. Social listening is a huge component of what the organisation does now in terms of outreach.

A participant wanted to know if specific messaging on Thunderclap could have been improved. A speaker replied that one of the challenges of National Preparedness Month every year is working with many stakeholders within and beyond the organisation, and inevitably, messages were not as focussed and consistent as expected. This was something that needed attention.

A participant wanted to know if FEMA worked with celebrities, and if so, what were the challenges and dynamics. A speaker replied that all government agency spokespeople must be credible in their own right. Notwithstanding, using celebrities to help has advantages too. The point is that one should use all tools at one's disposal to enhance public communications.

A participant wanted to know about how FEMA deals with negative perceptions and misinformation on social media. A speaker replied that there would always be trolls and/or people that one will never be able to convince no matter how much effort is put in. As such, it is better to focus on those one could reach.

A participant enquired if social media was making conspiracy theories worse. A speaker replied that as social media is a democratised media, everyone is their own media outlet now. It was inaccurate to think of the situation as an 'us versus the internet' or 'us versus people on Twitter', rather it is great to have robust and open discussions about a whole host of things, but there will ultimately be difficult folk out there.

A participant wanted to know how best to deal with misinformation, especially since it spreads very quickly. A speaker responded that the best way was to stay on top of the situation. It was important to constantly monitor what people were saying. One also needed to have an idea of what was undermining efforts. One had to be smart enough to figure out the real issues when dealing with disaster response. Most miscommunication and rumours were not an issue, but once they reached a certain level, one needed to figure out how to address them quickly.

A participant asked how ATHENA integrates online information to deal with crime. A speaker replied that the system uses an application called Hena which possesses live social media analytic capabilities. It targets suspects by going through social media footprints; it is able to detect suspects who have posted something or if they have been mentioned online. It has image processing capabilities as well. These data will then be mapped against existing criminal data such as DNA and CCTV records. It thus combines traditional investigative tools with new technology. It uses four basic scenarios: major burglary, human trafficking, counter-terrorism, and radicalisation.

A participant asked how ATHENA maps pictures of locations. A speaker replied that the system collected 20,000-40,000 tweets on social media related to ISIS, in 40 different languages. Depending on the type of platforms used, it can, for example, identify geo-tags of a user's location. Most people think terrorist groups are stupid to leave their footprints on social media, but the more intelligent terrorists no longer use the social media. They only use it for PR campaigns and recruitment. For operational purposes, they prefer to use gaming platforms to plan attacks. For example, they would use the chat feature within the gaming environment and the game characters to identify potential recruits. No law enforcement agency has

the capabilities to deal with this because no gaming organisation will provide a user's details unless you hack them yourselves in which case, you are breaking the law as well. It is also difficult to intercept because you do not know what you are intercepting, whether it is part of the game, or real-life terrorists in action. Far right terrorist groups, traditional Al Qaeda-inspired terrorist groups are using gaming platforms for recruitment and planning attacks.

A participant asked which social media platform provided the most information for analysts. A speaker replied that for ISIS, Twitter provides the most information. But the problem is that it is very easy for them to set up many accounts within a short period of time, which will then be shut down by Twitter. Collecting information within that short span of time before they are taken down is extremely challenging for analysts. For radicalisation purposes, Facebook yields the most information. Going back to an earlier point, gaming platforms are very useful for ISIS recruitment. Our study showed that the allure of gaming platforms for recruitment has nothing to do with religious ideology, but a lot to do with the allure of Hollywood-type action. For example, a study of the posture of ISIS fighters holding guns showed much similarity to Hollywood action films.

A participant asked about the future development of the ATHENA project. A speaker replied that a second sort of prototype would be launched in 2015. The advantages were that it was free, and members of the public could basically use the app without complications. Also, this prototype could be made available to every law enforcement agency or emergency services across the globe for free. In March 2015, major live exercises called 'Doomsday Scenarios' would be run. For example, an aircraft carrying biohazard material will fly over the city of Leeds and land in the city centre where a simulated terrorist attack would be carried out. The ATHENA app can help law enforcement agencies deal with such scenarios through its geo-location tagging and battle language management features. The app also empowers citizens in a less formal way as it allows them to ask for help quickly. It provides a universal emergency hotline.

A participant wanted to know if ATHENA was able to distinguish information from misinformation.

A speaker replied that ATHENA has a command/control dashboard which monitors everything that is related to a particular incident, it identifies the rumours and misinformation, and finally corrects such misinformation by disseminating the accurate information and counter-narrative. Timely information is very important to people, and it is acknowledged that they will trust the system more if it provides them with live incident updates.

A participant wanted to know if the use of Blackberry Messenger (BBM) by rioters during the London riots was unanticipated. A speaker replied that once the rioters learnt through the news that Twitter was the prime medium used during the riots, they switched to BBM. BBM has always been popular among gangs and those who have something against the government. At least 50 cases of BBM usage by rioters was seen during the riots. It is difficult to monitor BBM like Twitter as BBM is a closed system and is unique in that respect.

A participant observed that in terms of forensics, two major mobile phone companies have stated that they intend to make encryption more secure. This was met with some criticism from law enforcement as this can essentially compromise investigations and assist criminals. The participant wanted to know what impact this would have on mobile phone forensics. A speaker replied that some mobile phone companies did indeed provide very secure encryption for their phones. From a consumer standpoint, this was of course very good, but from a law enforcement perspective, more problems could actually be created. As to whether encrypting services were really effective, the speaker opined that many companies were simply engaged in marketing. For instance, one can find many decryption keys on the Internet even for seemingly encrypted apps.

DIALOGUE SESSION

Evolving Government Communications in Singapore

KU Menon, Senior Consultant, Ministry of Communications and Information



K U Menon

K U Menon began by discussing the historical context of how government communications in Singapore originated. Since the birth of the nation, it was deemed that norms relating to freedom of the press would have to be subordinate to Singapore's national interests. This paradigm detracted sharply from Western norms but was deemed appropriate at the time. In contemporary times, Singapore has entered the "post-deferential" age, where there is an emerging discourse that is somewhat at odds with Confucian values. Although social media seems to have gained much ground in recent times, the mainstream media is still dominant in Singapore. The key difference lies in mainstream media's traditional practice of editorial scrutiny, which is often absent in independent and online media.

It is crucial for government communications to evolve in light of the current trends. The government has been proactive in improving its communications strategy, and has moved into the online realm. The Prime Minister and several ministers have online presences via their Facebook pages or blogs for instance. Surveys have demonstrated that citizens do appear to be aware of policies and government initiatives as well as the plethora of online platforms that can be used to access government services. However, there are some areas that need improvement. These include better engagement of seniors, the young, and the educated.

In conclusion, Menon argued that government communication efforts should be cognisant of different contexts. He further stated that in spite of the rise in contending ideas, the values held by most Singaporeans remained largely unchanged. Citing an Institute of Policy Studies report, Menon highlighted how efficiency and good governance remained at the top of the list of societal values. This, Menon deemed, should be on the minds of stakeholders when approaching government communications.

Discussion

The discussion started with a question on how agencies could better engage the public. The speaker replied that providing sufficient civic space was one method. However, both the public and government should be circumspect so as to avoid conceding the discourse to a "hostile mob".

Another participant asked how the government viewed alternative media sites. The speaker replied that such sites were part of the new media landscape. He also cautioned that what is online is not necessarily true, and that the perceived volume of hostility may be weaker than thought.

A participant wanted to know about the challenges related to ministers' use of social media for public engagement. The speaker replied that due to the inherent complexities and dynamics of this space, public figures should be mindful of the pitfalls.

WORKSHOP AGENDA

Thursday, 27 November 2014 (Day 1)

0800 - 0845hrs Registration

Venue: Marina Mandarin Ballroom

Foyer (Level 1)

0845 – 0900hrs RSIS Corporate Video + Welcome

Remarks by Kumar Ramakrishna,

Head, Centre of Excellence for National

Security (CENS), RSIS

Venue: Marina Mandarin Ballroom

(Level 1)

Attire: Smart Casual (Long-sleeved

shirt without tie)

0900 – 1000hrs Keynote Address

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Kumar Ramakrishna, Head, Centre of Excellence for National Security (CENS),

RSIS

Speaker:

Too Much Digital Drama: Creating

A Better and More Productive
Approach to Online Discourse and

Conflict by Andrea Weckerle, Founder,

CiviliNation

Q & A

Venue: Marina Mandarin Ballroom

Foyer (Level 1)

1015 – 1215hrs Panel 1: Changing Perceptual

Behaviours

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Kumar Ramakrishna, Head, Centre of

Excellence for National Security (CENS),

RSIS

Speakers:

Misinformation and its Correction

in the Social Media Domain by

Ullrich Ecker, Associate Professor and Research Fellow of the Australian

ana Research Fellow of the Australian Research Council, School of Psychology,

The University of Western Australia

Effective Public Policy

Communication in the Age of Information Overload – The Role

of Imagery on Citizen Perception

and Compliance of Public Policy by

Michael J. Ahn, Assistant Professor,

Department of Public Policy and Public

Affairs, University of Massachusetts,

Boston

Understanding Social Media in

Singapore: Assumptions, Analyses,

Actions by **David Chan**, Lee Kuan

Yew Fellow & Professor of Psychology, Director, Behavioural Sciences Institute,

Singapore Management University

1215 – 1315hrs **Lunch**

Venue: Pool Garden (Level 5)

1315 – 1515hrs Panel 2: Public Trust in the Digital

Age

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Shashi Jayakumar, Deputy Head,

Centre of Excellence for National

Security (CENS), RSIS

Speakers:

Enhancing Trust in the Government

– Views from a former Nominated

Member of Parliament, by Eugene

Tan, Associate Professor of Law, Co-

Director, SMU Centre for Scholars'

Development, Singapore Management

University

Increasing Public Trust in the Social Media Age – Views from a Senior Communications Practitioner

by **Melvin Yuan**, Founder/Director, Omnifluence

Enhancing Trust in the Government

by **Mr Vikram Nair**, MP, Sembawang GRC and Vice-Chairman of Sembawang Town Council

Q & A

1515 - 1530hrs **Tea Break**

Venue: Marina Mandarin Ballroom

Foyer (Level 1)

1530 – 1730hrs Panel 3: Case Studies 1

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Caitríona H. Heinl, Research Fellow, Centre of Excellence for National

Security (CENS), RSIS

Speakers:

Correcting Misperceptions: What Works by **Jason Reifler**, Senior Lecturer of Politics, University of Exeter

NSW Police Force Use of Social Media by Strath Gordon, Director,

Public Affairs, NSW Police Force

Visual Propaganda in the Age of Social Media by Hyunjin Seo,

Assistant Professor and Docking Faculty Scholar, William Allen White School of Journalism and Mass Communications, University of Kansas

Q & A

1730hrs End of Day 1

1830 – 2030hrs Workshop Dinner (by invitation

only)

Venue: AquaMarine (Level 4)

Marina Mandarin Singapore

Friday, 28 November 2014 (Day 2)

0800 - 0845hrs Registration

Venue: Marina Mandarin Ballroom

Foyer (Level 1)

0845 – 1045hrs Panel 4: Tools for Social Media

Analysis

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Norman Vasu, Deputy Head, Centre of Excellence for National Security (CENS),

RSIS

Speakers:

Social Media Science: Implications

for Research, Analysis and

Policymaking by **Carl Miller**, Research Director, Centre for the Analysis of

Social Media (CASM), DEMOS, UK

TALISON - Tensor Analysis of Social

Media Data by **Anne Kao**, Senior Technical Fellow, Boeing Research &

Technology

EMBERS: Forecasting Civil Unrest using Open Source Indicators by

Brian Goode, Postdoctoral Research Associate, EMBERS Project, Discovery

Analytics Center, Virginia Tech

Q & A

1045 - 1100hrs Tea Break

Venue: Marina Mandain Ballroom

Foyer (Level 1)

1100 – 1300hrs Panel 5: Legal and Regulatory

Frameworks

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Bilveer Singh, Adjunct Senior Fellow, Centre of Excellence for National

Security (CENS), RSIS

Speakers:

The Problem of Regulating Open Source Intelligence Gathering in the United Kingdom by Simon McKay, Principal, McKay Law Solicitors & Advocates

Study, Search and Seizure in Social Media – The Legal and Regulatory

Benjamin Ang, Education Chair, The Internet Society (Singapore Chapter) and Lecturer, School of Business, Temasek Polytechnic

Framework in Singapore by

Developing a Regulatory
Framework for Social Media
Analysis and Investigation: Key
Components and Issues by Simon
Chesterman, Dean, Faculty of Law,
National University of Singapore

Q & A

1300 - 1400hrs Lunch

Venue: Pool Garden (Level 5)

1400 – 1600hrs Panel 6: Case Studies 2

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Norman Vasu, Deputy Head, Centre of Excellence for National Security (CENS),

RSIS

Speakers:

Using Social Media Analysis for Emergency Preparedness – FEMA's Experience by Rafael Lemaitre,

Director, Public Affairs, Federal Emergency Management Agency (FEMA) Application of Open Source Intelligence (OSINT) for Crisis Management: An Overview of the ATHENA Project by Babak Akhgar, Professor and Director of CENTRIC,

Sheffield Hallam University

Digital Forensics: Analysing Social Media Data on Mobile Devices by Christopher Church, Digital Forensic Specialist Digital Forensic Lab, INTERPOL Global Complex for Innovation, Singapore

Q & A

1600 – 1620hrs Networking Break

Venue: Marina Mandarin Ballroom

Foyer (Level 1)

1620 - 1700hrs **Dialogue**

Venue: Marina Mandarin Ballroom

(Level 1)

Chairperson:

Damien D. Cheong, Coordinator, Homeland Defence Programme and Research Fellow, Centre of Excellence for

National Security (CENS), RSIS

Speaker:

Inflection Point for Government Communications? by K U Menon, Senior Consultant, Ministry of Communications and Information,

Singapore

1700hrs End of Workshop

1815 – 2030hrs Closing Dinner (by invitation only)

Venue: Peach Blossoms (Level 5)

Marina Mandarin Singapore

LIST OF SPEAKERS AND CHAIRPERSONS

SPEAKERS

Michael J. Ahn

Assistant Professor

Department of Public Policy and Public Affairs

University of Massachusetts

Babak Akhgar

Professor and Director of CENTRIC

Sheffield Hallam University

Benjamin Ang

Education Chair, Internet Sociey (Singapore Chapter) Lecturer, School of Business, Temasek Polytechnic

David Chan

Lee Kuan Yew Fellow and Professor of Psychology Director, Behavioural Sciences Institute Singapore Management University

Simon Chesterman

Dean

Faculty of Law

National University of Singapore

Christopher Church

Mobile Forensics Specialist

INTERPOL

Ullrich Ecker

Assistant Professor

University of Western Austalia

Brian Goode

Post-Doctoral Associate

Discovery Analytics Center - Virginia Tech

Anne Kao

Senior Technical Fellow

Boeing Research & Technology

Rafael Lemaitre

Director

Federal Emergency Management Agency

Simon McKay

Principal

McKay Law Solicitors & Advocates

K U Menon

Senior Consultant

Ministry of Communications and Information

Carl Miller

Research Director

Centre for the Analysis of Social Media (CASM)

DEMOS

Vikram Nair

MP, Sembawang GRC

Vice-Chairman, Sembawang Town Council

Jason Reifler

Senior Lecturer of Politics

University of Exeter

Hyunjin Seo

Assistant Professor and Docking Faculty Scholar William Allen White School of Journalism and Mass Communications, University of Kansas

Eugene Tan

Associate Professor of Law

Co-Director, SMU Centre for Scholars' Development

Singapore Management University

Andrea Weckerle

Founder

CiviliNation

Melvin Yuan

Founder/Director

Omnifluence

CHAIRPERSONS

Damien D. Cheong

Coordinator, Homeland Defence

Programme and Research Fellow

Centre of Excellence for National Security (CENS)

S. Rajaratnam School of International Studies (RSIS)

Caitríona H. Heinl

Research Fellow

Centre of Excellence for National Security (CENS)

S. Rajaratnam School of International Studies (RSIS)

Shashi Jayakumar

Senior Fellow and Deputy Head Centre of Excellence for National Security (CENS)

S. Rajaratnam School of International Studies (RSIS)

Kumar Ramakrishna

Head

Centre of Excellence for National Security (CENS)

S. Rajaratnam School of International Studies (RSIS)

Bilveer Singh

Adjunct Senior Fellow

Centre of Excellence for National Security (CENS)

S. Rajaratnam School of International Studies (RSIS)

Norman Vasu

Senior Fellow and Deputy Head

Centre of Excellence for National Security (CENS)

S. Rajaratnam School of International Studies (RSIS)

ABOUT CENS

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.

Why CENS?

In August 2004 the Strategic Framework for National Security outlined the key structures, security measures and capability development programmes that would help Singapore deal with transnational terrorism in the near and long term.

However, strategising national security policies requires greater research and understanding of the evolving security landscape. This is why CENS was established to increase the intellectual capital invested in strategising national security. To this end, CENS works closely with not just other RSIS research programmes, but also national security agencies such as the National Security Coordination Secretariat within the Prime Minister's Office.

What research does CENS do?

CENS aspires to be an international research leader in the multi-disciplinary study of the concept of resilience in all its aspects, and in the policy-relevant application of such research in order to promote security within and beyond Singapore.

To this end, CENS conducts research in three main domains:

• Radicalisation Studies

The multi-disciplinary study of the indicators and causes of violent radicalisation, the promotion of community immunity to extremist ideas and best practices in individual rehabilitation.

Social Resilience

The inter-disciplinary study of the various constitutive elements of social resilience such as multiculturalism, citizenship, immigration and class. The core focus of this programme is understanding how globalized, multicultural societies can withstand and overcome security crises such as diseases and terrorist strikes.

· Homeland Defence

A broad domain researching key nodes of the national security ecosystem. Areas of particular interest include the study of strategic and crisis communication, cyber security and public attitudes to national security issues.

How does CENS help influence National Security Policy?

Through policy-oriented analytical commentaries and other research output directed at the national security policy community in Singapore and beyond, CENS staff members promote greater awareness of emerging threats as well as global best practices in responding to those threats. In addition, CENS organises courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

How does CENS help raise public awareness of National Security issues?

To educate the wider public, CENS staff members regularly author articles in a number of security and intelligence-related publications, as well as write op-ed analyses in leading newspapers. Radio and television interviews have allowed CENS staff to participate in and shape the public debate on critical issues such as radicalisation and counter-terrorism, multiculturalism and social resilience, as well as crisis and strategic communication.

How does CENS keep abreast of cutting edge National Security research?

The lean organisational structure of CENS permits a constant and regular influx of Visiting Fellows of international calibre through the Distinguished CENS Visitors Programme. This enables CENS to keep abreast of cutting edge global trends in national security research.

For more information about CENS, visit http://www.rsis.edu.sg/cens

ABOUT RSIS

The **S. Rajaratnam School of International Studies (RSIS)** was officially inaugurated on 1 January 2007. Before that, it was known as the Institute of Defence and Strategic Studies (IDSS), which was established ten years earlier on 30 July 1996. Like its predecessor, RSIS was established as an autonomous entity within Nanyang Technological University (NTU). RSIS' aim is to be a leading research institution and professional graduate school in the Asia Pacific. To accomplish this mission, RSIS will:

- · Provide a rigorous professional graduate education in international affairs with a strong practical and area emphasis
- Conduct policy-relevant research in national security, defence and strategic studies, international political economy, diplomacy and international relations
- · Collaborate with like-minded schools of international affairs to form a global network of excellence

Graduate Education in International Affairs

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The teaching programme consists of the Master of Science (M.Sc.) degrees in Strategic Studies, International Relations, International Political Economy and Asian Studies. Through partnerships with the University of Warwick and NTU's Nanyang Business School, RSIS also offers the NTU-Warwick Double Masters Programme as well as The Nanyang MBA (International Studies). Teaching at RSIS is distinguished by its focus on the Asia Pacific region, the professional practice of international affairs and the cultivation of academic depth. Over 230 students, the majority from abroad, are enrolled with the School. A small and select Ph.D. programme caters to students whose interests match those of specific faculty members.

Research

Research at RSIS is conducted by six constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS); the International Centre for Political Violence and Terrorism Research (ICPVTR); the Centre of Excellence for National Security (CENS); the Centre for Non-Traditional Security (NTS) Studies; the Temasek Foundation Centre for Trade & Negotiations (TFCTN) and the Centre for Multilateralism Studies (CMS). The focus of research is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region. The School has four endowed professorships that bring distinguished scholars and practitioners to teach and do research at the School. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, the NTUC Professorship in International Economic Relations and the Bakrie Professorship in Southeast Asia Policy.

International Collaboration

Collaboration with other professional schools of international affairs to form a global network of excellence is an RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

For more information about RSIS, visit http://www.rsis.edu.sg

ABOUT NSCS

The **National Security Coordination Secretariat (NSCS)** was set up in the Prime Minister's Office in July 2004 to facilitate national security policy coordination from a Whole-Of-Government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is Deputy Prime Minister and Minister for Home Affairs Mr Teo Chee Hean.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS (NSIC) is Mr Benny Lim, who is concurrently Permanent Secretary (National Development) and Permanent Secretary (Prime Minister's Office).

NSCS comprises two centres: the National Security Coordination Centre (NSCC) and the National Security Research Centre (NSRC). Each centre is headed by a Senior Director.

The agency performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipation of strategic threats. It also organises and manages national security programmes, one example being the Asia-Pacific Programme for Senior National Security Officers, and funds experimental, research or start-up projects that contribute to our national security.

For more information about NSCS, visit http://www.nscs.gov.sg/



