SOCIAL MEDIA AND DIGITAL MATURITY: IMPLICATIONS FOR NATIONAL SECURITY

31 OCTOBER – 1 NOVEMBER 2013, SINGAPORE

SOCIAL MEDIA AND DIGITAL MATURITY: IMPLICATIONS FOR NATIONAL SECURITY

CONTENTS PAGE

This report summarises the proceedings of the workshop as interpreted by assigned rapporteurs and editor of the S. Rajaratnam School of International Studies. Participants neither reviewed nor approved this report.

The workshop adheres to a variation of the Chatham House Rule. Accordingly, beyond the points expressed in the prepared papers, no attributions have been included in this workshop report.

EXECUTIVE SUMMARY

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

In his opening remarks, **Kumar Ramakrishna** discussed the importance of social media analytics and digital maturity in relation to the burgeoning of social media usage. With approximately 2.4 billion people online and using social media extensively, lines between the real and the online realm have become blurred. In this context, social media could offer opportunities for national security but could also pose challenges. Some of these challenges are: (a) social media could provide a forum for online radicalisation; (b) controversial online debates, hate speech and incitement to violence could escalate and manifest in the physical world, thereby causing social disturbances and crises; and (c) social media could provide a communication and organisation platform that facilitates real-world activity (e.g. riots). At the same time, social media could also be employed to aid national security efforts such as crisis management, threat reduction, surveillance, and overall public engagement. Given the growing importance of social media to national security efforts, Ramakrishna observed that social media analytics had become an important feature of the national security landscape. He argued, however, that harnessing this new technology must be accompanied by the enhancement of digital maturity, that is, how people evaluate the information they receive from online sources. He concluded that the workshop aimed to facilitate discussions on social media analytics and digital maturity from multidisciplinary perspectives.

Panel 1: Social Media Analytics: Social Media Analytics in Investigation and Analysis

Defending the Realm using Social Media Analytics
Alan Jenkinson, Director of Strategic Business – Home and Foreign Affairs at Hewlett-Packard

Alan Jenkinson discussed the UK government's approach to social media analytics *vis-a-vis* the defence of the realm. He observed that data fusion and analytics would allow law enforcement to optimise its decision-making process and provide additional support through higher level of effectiveness, agility and efficiency. He also identified related challenges such as compliance with legal regulations, storage of data and data security. He predicted that as human information was changing drastically and rapidly, the analytics industry would move on to more meaning-based computing. This was defined as the development of algorithms to analyse information similar to that of the human brain. The UK government's data analytics doctrine, he explained, used data from past events (hindsight), data fusion and analytics to develop insights that would allow for better foresight of future events. Jenkinson underscored the importance of educating and training senior officials and staff as big data processing needed better decision-making capabilities.

The Facebook Effect: A Law Enforcement Perspective
Nick O'Brien, Associate Professor Counter Terrorism and Head of School, Australian Graduate School of Policing and Security, Charles Sturt University

Nick O'Brien discussed the implications of the proliferation of online social networks on law enforcement. He argued that the convergence of new technologies such as facial recognition, cloud computing and mobile technologies with social networks, created new challenges as well as opportunities for governments and law enforcement. The main challenges included: (a) prevalence of "assumed identities"; (b) ethical issues; and (c) data privacy issues. He identified the key opportunities as: (a) possibility of tracking individuals; (b) intelligence-gathering from social networking sites; and (c) tracking of mobile phones using geolocator applications.

Using Social Media Analytics in Investigation and Analysis – Current Issues and Future Trends
Stephen Tracy, Insight & Analytics (I&A) Lead for APAC, Waggener Edstrom

In his presentation, **Stephen Tracy** discussed the major challenges facing the analytics industry, current trends impacting the industry, and how the industry was driving innovation and new capabilities in social listening technologies. Tracy then discussed how governments and the private sector could collaborate more effectively

in the field of social media analytics. He suggested that collaboration could be done in terms of: (a) research and discovery; (b) crisis identification and response planning; (c) development of crisis systems; and (d) development of best practices for government monitoring and engagement.

Panel 2: Social Media Analytics: New and Emerging Technologies

[SKYPE Presentation] GDELT: Realtime Automated Global Behavior and Beliefs Mapping, Modelling, and Forecasting Using Hundreds of Millions of Events
Kalev H. Leetaru, Yahoo! Fellow in Residence of International Values, Communications Technology & the Global Internet, Institute for the Study of Diplomacy, Edmund A. Walsh School of Foreign Service, Georgetown University

Kalev Leetaru's presentation discussed the Global Database of Events, Language, and Tone (GDELT) initiative. GDELT is an on-going initiative that attempts to construct a catalogue of human societal-scale behaviour and beliefs across all countries of the world. The data is freely available and comprises information over the last two centuries. Daily updates are provided in order to create the first "real-time social sciences earth observatory". GDELT's main objective is to assist in the uncovering of previously obscured spatial, temporal, and perceptual evolutionary trends through new forms of analysis of the vast textual repositories that capture global societal activity, from news and social media archives to knowledge repositories. GDELT's evolving ability to capture religious, ethnic and other cultural and social group relationships is envisaged to offer new insights into the interplay of those groups over time. This is expected to offer a rich platform for understanding patterns of social evolution. Also, the data's real-time nature is expected to expand current understanding of social systems beyond static snapshots and take into account the non-linear behaviour and feedback effects that define human interaction. In doing so, fragility indexes, early warning systems, and forecasting efforts would be enriched.

Making Sense of Social Media: Who, What, How
Carol Soon (with contributions from Marc Smith), Research Fellow, Institute of Policy Studies, NUS

Carol Soon's presentation focused on the use of NodeXL, a social media network analysis tool that enables the analysis of Twitter conversations. The tool is premised on the use of social network theories, which essentially underpins the study of social structures formed from the aggregate of relationships amongst a population. Identifying the nodes (actors) and edges (relationships connecting the nodes) are important as is the analysis of key network metrics such as centrality, cohesion and density, which would enable analysts to identify key influences. NodeXL is an open-source social network analysis add-in for Microsoft Excel 2007 and 2010, leveraging a spreadsheet as a host for social network analysis. Data collected on nodes and their relationships are contained in excel sheets and upon the completion of the analysis, the tool allows for visualisation of the networks. The algorithm contained in NodeXL essentially places each person in a group based on how densely people who are tweeting about a topic are connected with each other. This captures a range of qualities about the location and connection patterns of each user within the larger network. Insights into how Twitter is used can be discerned through different types of social media network patterns.

Social Hacking and Cognitive Security
Rand Waltzman, Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)

Rand Waltzman discussed the vast potential provided by the internet and social media to influence individuals online. He also discussed some of the current approaches being developed to guard against negative influencing.

Social Analytics using Twitter Data
Lim Ee Peng, Professor of Information Systems, Co-Director, Living Analytics Research Centre, Singapore Management University (SMU)

Lim Ee Ping discussed several social media analytics research projects that were currently being undertaken at the Living Analytics Research Centre, a collaborative project between the Singapore Management University (SMU) and the Carnegie Mellon University (CMU). An

analytics tool developed by LARC is Palanteer. Palanteer employs a unique framework for gathering and searching microblog data by focusing on harvesting community-relevant content. It uses a timeline-based interface and word cloud visualisation to enable the researchers to explore and make sense of temporally-relevant information. The framework is customisable, and can be used to create search engines for different community of users and microblogging sites. Lim then provided a live demonstration of Palenteer.

Distinguished Lunch Lecture

Legal Implications of Employing Social Media Analytics
Rebecca Weiner, Director of Intelligence Analysis, New York Police Department (NYPD)

Rebecca Weiner first discussed how terrorist activity was being conducted online. She then provided an overview of how the New York Police Department (NYPD) uses social media to support its investigations. She also discussed the evolving legal architecture that governed law enforcement's use of social media, and identified several key challenges of doing so, such as the necessity to balance operational needs with protection of privacy and transparency.

Panel 3: Social Media Analysis – Key Issues

Psychological Considerations for Digital Maturity: What are the Security Challenges and Implications?
Majeed Khader, Director, Behavioural Science Unit, Home Team Academy (HTA)

Majeed Khader discussed: (a) how the digital age had impacted lifespans; (b) why attention must be paid to digital maturity in the same way attention was paid to other areas of human maturity (e.g. physical development, behavioural development, emotional development, social development and cognitive maturity development); and (c) emerging concerns from the security and resilience perspectives. Khader proposed several initiatives to address these concerns including: (a) the development of virtual immune systems and cyber resilience through: (i) fostering childrens'"virtual immune systems"; (ii) nurturing children online and offline; (iii) monitoring internet addiction; and (iv) paying attention

to older children; (b) the need to study more closely the link between internet deviance, cybercrime and human interface; (c) fine-tuning legislation and law enforcement policies for the digital age; and (d) developing new ways to leverage the internet for positive outcomes.

Managing the Risks of Social Media in the SAF
Sam Lee Hsiang Wei, Republic of Singapore Air Force

Sam Lee Hsiang Wei argued that the Singapore Armed Forces (SAF) faced five key risks as it moved to embrace the social media phenomenon: (a) risk through direct disclosure; (b) risk through revealing locations; (c) risk through user anonymity; (d) risks by design; and (e) risk from information aggregation. This was due in part to the inevitable blurring of the servicemen/women's personal and professional capacities. As such, Lee proposed a three-pronged approach – education, clear boundaries/guidelines and support processes – that would enable personnel to continue using social media in their personal capacity without posing undue risks to the SAF.

Panel 4: Case Studies

The Role of Social Media in the Response to the Boston Marathon Attacks
John Daley, Chief Technology Officer and Deputy Superintendent, Boston Police Department

John Daley highlighted the importance of police departments remaining active on social media, particularly during a crisis. Daley spoke of his own experience in the Boston Police Department (BPD) before the Boston Marathon Bombing on 15 April 2013. He noted that in 2008, the BPD was engaged in online conversations with the general public on Twitter as it provided a forum for people to make complaints and comments to the BPD. The BPD also created their own website with timely announcements on changes that would affect the day-to-day lives of the general public, such as road closures. During the Boston Marathon bombing the BPD capitalised upon its existing online presence not only to instruct people on how to respond to the attack, but also to facilitate the exchange of information that could help with on-going investigations. Daley noted that the BPD follows four guiding principles for interaction on social media: (a) integrate it into everyday business – from routine to critical; (b) utilise dialogue as well as

other broadcasting media; (c) expand responsibility for communications beyond public information officers; and (d) listen to what people are saying and respond accordingly.

Social Media Intelligence – Lessons Learnt
Daniel Pearce, Head of Analysis, Open Source and Social Media, Metropolitan Police Service

Daniel Pierce discussed his experience during the London Olympics in 2012 as Head of the London Metropolitan Police All Source Hub. He stated that the London Olympics was the largest social media event of all time, and required 24-hour monitoring online and extensive filtering of Facebook and Twitter posts using 20 000 key-word searches. This resulted in 31 million security relevant posts online and 2562 intelligence reports. Pierce spoke of the many lessons learnt by the London police during the Olympics, one of which was not to assume that senior officials and politicians understood social media and the intelligence that it could provide security officers, and consequently, not to expect that they would devote adequate attention or resources to its study. Pierce drew attention to the array of challenges for social media intelligence analysis, which included the considerable number of staff required to sift through the significant amounts of data, as well as the legal complications surrounding data privacy and intentional misinformation.

CERA's use of Social Media Analytics for Disaster/ Emergency Operations
Mike Shatford, Deputy Chief Executive, Communications, Canterbury Earthquake Recovery Authority (CERA)

Mike Shatford spoke of his experience during the Canterbury earthquake in New Zealand on 4 September 2010, as well as the subsequent aftershocks – the most destructive one occurring on 22 February 2011. He described the widespread damage caused to Christchurch including infrastructure, sewerage and telecommunications. The scale of the disaster meant that overall recovery required integrated and timely decision-making across a range of organisations. It was for this reason that the Canterbury Earthquake Recovery Authority (CERA) was established in early 2011. CERA had a local focus, and took on a leadership and facilitation role. It focussed on responding, rebuilding and recovering, and used social media platforms that were trusted by the public and well-maintained for those ends.

Shatford maintained that governments should have a coordinated crisis plan across agencies. He also suggested that alternative methods of communication should be established since social media channels could easily be broken if power lines were destroyed in a disaster. He observed that building trust between the government and the community was very important during a crisis, and this could only be accomplished through the provision of reliable, verifiable and immediate information.

Morning Lecture

Social Media and The Arab Spring – Tweeting the Uprisings
Nasser Weddady, Outreach Director, American Islamic Congress (AIC)

Nasser Weddady's presentation focussed on the behind-the-scenes role of activists in the Arab Spring uprisings. He argued that the social network of activists and their communication strategies were the main drivers of the Arab Spring rather than social media activism as had been previously argued. The network of activists in the Arab world, according to Weddady, worked closely to translate online activism into political mobilisation in the real world. To this end, the activists employed two broad communication strategies: (a) cross-posting for advocacy and weaving various online platforms together to maximise the campaign outreach; and (b) crafting the message in a way that could make sense to both local and international media. They also linked local activists to international media, which enabled them to shape the narrative pertaining to the uprisings. Weddady reiterated that the success of political mobilisation that led to the Arab Spring was influenced not by the power of social media *per se* but the human activists driving it.

Panel 5: Efforts to Improve Digital Media Literacy

Singapore's Media Literacy Council – 1 Year On
Lai Lei Khim, Executive Director, Media Literacy Council

Lai Lei Khim first gave an overview of the changing internet landscape and its potential threats. She then discussed the reasons for the formation of the Media Literacy Council (MLC), and outlined its main vision – "Discerning Singaporeans who are able to evaluate

media content effectively, and to use, create and share content safely and responsibly". To achieve this, the MLC collaborates with "industry, community and government to promote an astute and responsible participatory culture". Several programmes and initiatives were also discussed. A key takeaway was that parents, educators and netizens had a major role to play in promoting media literacy and digital citizenship.

Enhancing Access and Use of Media and ICTs through Media and Information Literacy
Alton Grizzle, Programme Specialist, Communication and Information Sector (CI), UNESCO

Alton Grizzle discussed UNESCO's efforts to improve the access and use of media and information literacy (MIL). He suggested four complementary strategies in order to make MIL a mass engaging civic education movement. These strategies include: (a) common curriculum for media literacy, (b) effective policies and strategies; (c) assessment framework; and (d) networking and global partnerships. Grizzle also argued that the negative

aspects of social media could not and should not always be addressed through legal measures, but rather through the development of media literacy skills especially among younger users.

Facing Online Hate: A Canadian Approach
Matthew Johnson, Director of Education, MediaSmarts, Canada

In presenting the Canadian approach to facing hate speech online, **Matthew Johnson** first shared MediaSmarts definition for online hate. He then proceeded to discuss why MediaSmarts had chosen to focus on youth as its main target group. Lastly, he presented several strategies to develop critical thinking and how to evaluate media content more effectively. These included: (a) teaching youth to develop empathy; (b) educate youth about the techniques that hate groups employ to support their arguments; (c) intervention; (d) reporting hate media to service providers (e.g. YouTube); (e) awareness-raising campaigns; and (d) related training for children, teenagers, parents and teachers.

WELCOME REMARKS

Opening Remarks
Kumar Ramakrishna, Head, Centre of Excellence for National Security (CENS), RSIS/NTU

Kumar Ramakrishna

Kumar Ramakrishna situated the importance of social media analysis and digital maturity in the context of the social media phenomenon now engulfing the world. 2.4 billion people were now online, and were highly active on social media platforms notably Facebook,

YouTube and Twitter. This has revolutionised the way individuals live to the extent that experts now claim that a "Digital You" exists. The blurring of lines between the real and online worlds has also occurred as a result, with "online" becoming an intimate, technologically-enhanced extension of each individual. While the internet and the explosive growth of social media has increased people-to-people linkages and has brought about many positive social, cultural and economic benefits, the negative dimension of this phenomenon must be acknowledged.

In the context of national security, increased social media usage can generate both positive and negative outcomes. For instance, new security challenges could be created such as: (a) online radicalisation; (b) escalation of real-world crises; (c) social disturbances; and (d) facilitation of hate speech and incitement to violence. A case in point was the deliberately miscaptioned images related to the Muslim-Buddhist conflict in the Rakhine state of Myanmar, which were disseminated through various

social media platforms. Such images motivated some extremist groups in Southeast Asia to mobilise volunteers to fight in Myanmar.

At the same time, social media could also be used positively by assisting national security efforts in the fields of: (a) crisis management; (b) threat deduction; and (c) overall public engagement. Initiatives are increasingly been made to leverage social media for investigation, analysis work, crisis management and event prediction. In light of these new developments, Ramakrishna observed that social media analytics was becoming an important feature of the national security landscape. He remarked that while useful to national security efforts, social media analytics had also raised concerns with regards to the ethical use of this technology. Ramakrishna also argued that as far as national security was concerned, harnessing social media technology was only one part of the equation. An equally important task for security experts and practitioners was to understand how people process, make sense of and evaluate the information they receive from online sources.

It was for this reason that the workshop would focus not only on social media analytics but also on digital maturity or the ability to rationally and critically evaluate information from online sources.

With the contributions of eminent speakers from Singapore and overseas, the workshop aimed to address three main questions: (a) how could practitioners use social media analytics practically, legally and effectively in investigation and analysis?; (b) what were the key issues to consider when employing social media in national security crisis mitigation?; (c) how could digital maturity help people become relatively more relational producers and consumers of content on social media platform; and (d) what could be done to promote such digital maturity? The various panels would discuss different topics such as the use of social media analytics in investigation and analysis; new and emerging technologies related to social media analytics; key issues in social media analytics; and empirical examples of the usage of social media analytics. In closing, Ramakrishna encouraged the participants to engage with the speakers and wished them a stimulating workshop.

SOCIAL MEDIA ANALYTICS: SOCIAL MEDIA ANALYTICS IN INVESTIGATION AND ANALYSIS

Defending the Realm using Social Media Analytics
Alan Jenkinson, Director of Strategic Business – Home and Foreign Affairs, Hewlett-Packard

Alan Jenkinson

Alan Jenkinson discussed the UK government's approach to social media analytics *vis-a-vis* the defence of the realm. He identified two major challenges that were confronting governments with regard to analysing big data. The first was the enterprise challenge, which created a highly complex environment for combining and analysing open source data with government-originated data. Second, the open source challenge. This referred to the ever-increasing volume and availability of data from open sources that made analysis more difficult.

Jenkinson then explained that although the government and private sector used the same social media analytical tools, they had very different objectives. The private sector often used such tools for marketing/branding campaigns, whereas the government used them in policy making, intelligence optimisation, crime reduction strategy campaigns and public engagement on policy issues. He opined that data fusion and analytics would allow law enforcement to optimise its decision support through higher levels of effectiveness, agility and efficiency, but also identified related challenges such as compliance with legal regulations, storage and data security.

Jenkinson also predicted that as human information was changing drastically and rapidly, the analytics industry would move on to more meaning-based computing, which was the development of algorithms to analyse information like the human brain.

The UK government's data analytics doctrine, Jenkinson explained, used data from past events (hindsight), data fusion and analytics tools to develop insights that would allow for better foresight about future events. Jenkinson concluded by underscoring the importance of educating and training senior officials and staff as big data processing needed better decision-making capabilities.

The Facebook Effect: A Law Enforcement Perspective
Nick O'Brien, Associate Professor Counter Terrorism and Head of School, Australian Graduate School of Policing and Security, Charles Sturt University

Nick O'Brien

Nick O'Brien discussed the implications of the proliferation of social networking sites on law enforcement. He argued that the convergence of new technologies such as facial recognition, cloud computing and mobile technologies with social networking sites created new challenges as well as opportunities for governments and law enforcement. The main challenges included: (a) prevalence of "assumed identities"; (b) ethical issues; and (c) data privacy issues, while the key opportunities were identified as: (a) possibility to track individuals; (b) intelligence gathering from social networking sites; and (c) tracking of mobile phones using geo-locator applications.
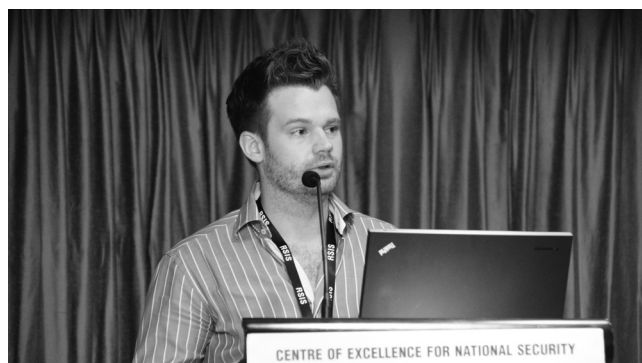
O'Brien started his presentation by discussing case studies of how the increased usage of social networking sites had impacted individuals' lives; from Al-Shabab communicating through its Twitter account, to the announcement of the end of the Libyan war on Facebook.

He argued, however, that linking new technologies to social media would give governments and private entities a very powerful and dangerous tool. In support of this view, O'Brien cited an example of how the use of facial recognition software on Facebook could easily identify users in a matter of seconds. O'Brien contended that the application of such technology in public would inevitably raise significant ethical issues and privacy concerns.

The easy access to cloud powered technologies was also a cause of concern as criminals and/or terrorists could easily buy cloud powered capacities on commercial servers such as Amazon. Furthermore, the prevalence of using social networking sites on smart phones and tablets was another emerging threat in terms of data privacy and individual security as it was now relatively easy to track users. Nevertheless, O'Brien argued that new technologies could still be employed for good in terms of aiding governments to neutralise security threats.

Using Social Media Analytics in Investigation and Analysis – Current Issues and Future Trends
Stephen Tracy, Insight & Analytics (I&A) Lead for APAC, Waggener Edstrom

Stephen Tracy

Stephen Tracy discussed the major challenges facing the analytics industry, current trends affecting the industry and how the industry was driving innovation and new capabilities in social listening technologies. Tracey then discussed how governments and the private sector could collaborate more effectively in the field of social media analytics.

Tracy identified vendor proliferation and mergers as the most noteworthy trends in the analytics industries over the past decade. He argued that all analytics tools were merely efficiency tools that could collect massive amount of data quickly but still needed the human element to deliver insight. According to Tracy, keyword profiling and web crawling, which enables users to understand the structure of a website and pull out information, were two common features of almost all social media listening tools.

Tracy then identified three core features of these tools: (a) automated sentiment analysis – the process of determining the implied tone of author of a social mention through natural language processing; (b) filtering – the ability to filter data by various criteria, such as region, date, channel type, sentiment, etc.; (c) classification – the ability to categorise social conversations or mentions by channel or channel types (e.g. social networking, microblogs, blogs, etc.); (d) data visualisation – the ability to visualise large volumes of data collected into a single dashboard; (e) engagement and workflow – features that allow one to engage (i.e. respond) directly to social mentions within the tool, as well as the ability to assign priority and respond to different team members; and (f) alerts – the ability to setup automated alerts that notify one of potential issues (or opportunities) based on pre-determined rules or criteria (e.g. conversation volume threshold, keyword rules, etc.).

He also briefly explained the application of qualitative analysis for gauging public perception and potential influencers, and quantitative analysis for early warning, crisis anticipation and real-time monitoring. Tracy contended that given the analytics industry's heavy investment on sentiment analysis and natural language processing and its substantial research capacity, the industry could collaborate with the public sector in terms of: (a) research and discovery – gauging public perception; (b) crisis identification and response planning – collaborating on the development of plans, protocols and frameworks for crisis management; (c) development of crisis systems – building government platforms for monitoring and response; and (d) development of government monitoring and engagement best practices – most of the best practices related to monitoring and outreach have been drafted for the private sector and there was a need to develop tailored best practices that suit the requirements of the public sector.

Discussion

A participant observed how social network analytics used to investigate an event, such as the Arab Spring uprisings, merely focused on the number of followers in social networks, while there were influencers in the real world who did not have a lot of followers but still commanded much influence. A panellist replied that the private sector was interested in measuring influence primarily from digital footprints (quantitative approach). He agreed that a qualitative approach to examine how influencers built a community around as well as gained authority both in the digital and physical domain was also needed to develop a better understanding.

Another participant questioned the accuracy and authenticity of information provided by social networks, and asked if there were any tools to verify information for accuracy. A panellist believed that the public were usually reactive to information due in part to their personal predispositions, which made them more likely to believe in inaccurate information and/or misinformation. The authorities were in a better position to verify information, and hence, could correct misinformation and dispel rumours. Another panellist added that the dissemination of misinformation, such as in the case of the Boston Bombing, in which an individual was incorrectly identified by netizens as being the bomber, was indeed challenging and dangerous. He replied that he was unaware of any information verification tool, and agreed that it was the human analysts that were most important in providing insights.

SOCIAL MEDIA ANALYTICS:
NEW AND EMERGING TECHNOLOGIES

GDELT: Realtime Automated Global Behavior and Beliefs Mapping, Modeling, and Forecasting Using Hundreds of Millions of Events
Kalev H. Leetaru, Yahoo! Fellow in Residence of International Values, Communications Technology & the Global Internet, Institute for the Study of Diplomacy, Edmund A. Walsh School of Foreign Service, Georgetown University

Kalev Leetaru's presentation focused on the potential use of big data in enhancing current understanding of human societies. With the advent of the internet and the current widespread use of social media, there was an exponential rise in data documenting today's human societies. At present, a third of the human population had a presence online. There are now as many cell phones as there are people on earth. Facebook has revealed that it now has over one billion members with one trillion connections. Every minute, 600 new websites are created and 204 million emails are sent worldwide. Hence, rich interconnections between societies exist online, and can provide important contextual background information on the patterns of human behaviour. Of further significance was the fact that for the first time, it was now possible to leverage computing power to process data from these online sources.

To tap into these rich sources of societal information, an initiative known as the Global Database of Events, Language, and Tone (GDELT) was set up. The GDELT is an initiative to construct a catalogue of human societal-scale behaviour and beliefs across all countries of the world over the last two centuries down to the city level globally, to make all of this data freely available for open research, and to provide daily updates to create the first "real-time social sciences earth observatory". Nearly a quarter-billion geo-referenced events capture global behaviour in more than 300 categories from 1979 to the present with daily updates.

The objective of the GDELT project is to monitor and process all news and social media worldwide into a single media catalogue of behaviour and beliefs globally, providing the first "real time social sciences earth observatory". Essentially the project uses the large archive of text and news media available numbering a quarter of a billion geo-referenced events and turns it into a massive quantitative database.

One of the obvious challenges faced by the project is the capacity and ability to process the huge volumes of data. The GDELT project uses tools such as Google's Big Query database service to interactively map events in seconds. In addition, the development of the GDELT Global Knowledge Graph allows researchers to go beyond events and to produce a single global graph connecting incidents such as people, organisations, themes and set events. For example, the database is able to focus on a political leader and produce graphs on how the global media has portrayed him within a given time frame. In conclusion, the GDELT project aims to uncover previously obscure spatial, temporal and perceptual trends, paving the way for new ways of analysing and comprehending human societies.

Making Sense of Social Media: Who, What, How
Carol Soon (with contributions from Marc Smith), Research Fellow, Institute of Policy Studies, NUS

Carol Soon

From a vast sea of tweets, posts, blogs and updates, social scientists are currently attempting to bring into clearer focus the wealth of human communication and interactions that occur through computer-mediated platforms. In this context **Carol Soon's** presentation focused on the use of NodeXL, a social media network

analysis tool that enables the analysis of Twitter conversations. The tool is premised on the use of social network theories, which essentially underpins the study of social structures formed by the aggregate of relationships amongst a population. Identifying the nodes (actors) and edges (relationships connecting the nodes) are important as is the analysis of key network metrics such as centrality, cohesion and density, which would enable analysts to identify key influences.

NodeXL is an open-source social network analysis add-in for Microsoft Excel 2007 and 2010, leveraging a spreadsheet as a host for social network analysis. Data collected on nodes and their relationships will be contained in excel sheets, and upon the completion of the analysis, the tool allows for visualisation of the networks. The algorithm contained in NodeXL essentially places each person in a group based on how densely people who are tweeting about a topic are connected with each other. This captures a range of qualities about the location and connection patterns of each user within the larger network. Insights into how Twitter is used can be discerned through different types of social media network patterns. For example, a "polarised" network often exhibits ongoing discussions between two big and dense groups with little connections between them with topics likely being the most contentious socially or politically. A "bazaar" network suggests that some popular topics may attract smaller groups which often form around a few hubs, each with its own audience, influencers and sources of information. A "broadcast" network represents patterns of most major news media outlets. They have a distinctive hub and pattern with people retweeting news feeds, thereby forming separate and distinct audience groups.

With the use of tools such as NodeXL, it is possible to collect and analyse social networks formed among people who tweet a common hashtag or phrase. Network measures identify people who occupy strategic positions at various positions within the network, enabling the analysis of people who are most popular or potentially most influential in a community. As more discussions move online, such tools can shed light on how conversations take place and the sources of important and influential contributions in a given society.

Social Hacking and Cognitive Security
Rand Waltzman, Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)

Rand Waltzman

Rand Waltzman's presentation began with a brief introduction to the Defence Advanced Research Projects Agency (DARPA). DARPA is an autonomous agency within the United States Department of Defense that funds a variety of research projects. DARPA is credited with the development of the internet, which was originally known as the ARPANET. At present, DARPA was interested in research surrounding new technology for the analysis of group dynamics and social media.

For Waltzman, the high velocity and reach of social media today has changed the constraints of group formations in fundamental ways. The groups on social media often form and mobilise quickly around a specific topic or for a particular purpose. However, the shallow bonds of group members imply that they could disband as quickly as they form. As such, an area of particular interest was group detection through a fusion of topic-based modelling and topological information. Also being considered were unique ways of trying to integrate dynamic models of competitive information diffusion in groups together with entropy based models for determining prolific users.

To illustrate, Waltzman discussed how "between a centrality" calculations could be used as a means of locating influential users. The technique does, however, contain several flaws, particularly in terms of analysing static networks. One such flaw is that for large graphs, the calculations used have been found to be unstable wherein missing links could change the values radically. Secondly, static networks are not capable of revealing

the entire picture of group formation; for more complete analyses what is needed is dynamic information from networks. The capture of group dynamics is therefore necessary to understand what is occurring.

Defining an online group as an evolving community of social media users that discusses an evolving set of topics, Waltzman noted that an important point to remember was that such groups could exist at 'multiple levels of extraction'. These different levels could range from broad-based topics with long term discussions to narrow topics with long-term discussions and/or to narrow topics with short term discussions. Often at times, one or more memes can be associated with such groups. While narrowly associated with a word or phrase in the commercial sectors, memes can now refer to concepts. Hence, recent research might be able to leverage on this development whereby a whole cluster of tweets can represent a linguistic instance of a specific concept. In conclusion, Waltzman predicted that while these new initiatives were not commercially available, they would radically change the landscape when made available in the future.

Social Analytics using Twitter Data
Lim Ee Peng, Professor of Information Systems, Co-Director, Living Analytics Research Centre, Singapore Management University (SMU)

Lim Ee Peng

In his presentation on social analytics using Twitter data, **Lim Ee Peng** noted that at present, social media involved many different people coming together to share ideas and generate content together. Introducing the research that was currently undertaken by the Living Analytics Research Center (LARC) of the Singapore Management University, Lim was of the view that one of the key

challenges faced was how to deal with the vast amount of data that was being generated online.

On average, nearly 1.5 million tweets are generated by Singaporean users per day, more than 30 million tweets per month. However, during events/crises, such as the recent cross-border haze from Indonesia, the number of tweets generated increases exponentially. Also, the speed at which the data was generated was extremely fast, and there was a lot of noise from "trolls", which had to be filtered out. Another challenge related to the issue of big data was storage. Lim noted that while there were ways to store such data, this might not be possible all the time.

Discussing the current research initiatives at LARC, Lim explained that 'crawlers' are used to collect data, which are then stored on a database. Search methods are then developed to mine and analyse the information. LARC has developed tools such as a twitter search engine and the Palanteer social analytics search engine, which enables real-time analysis. The tweets gathered would allow researchers to analyse the latest trends in societies, determining frequently used keywords as well as users and pictures that are cited often.

In conclusion, Lim was of the view that while social media presents unparalleled opportunities for researchers and social scientists, the main challenge was to manage the glut of messy and noisy real-time data. New directions for research included initiatives to integrate different social media platforms as well as including more context-aware methods for analysing social media. The development of new research techniques and tools would invariably be needed to keep abreast of the constantly changing online environment.

Discussion

A participant asked how data cleaning was done to remove the noise from the large amount of data prior to the advent of tools such as NodeXL. A speaker responded that traditionally, commercial data cleaning tools that allowed for filtering of collected data were used. However, there was a need for domain expertise and human analysis in determining that the data collected was relevant for analysis.

Another participant inquired as to why social media in Singapore was used more to broadcast instead of engaging in conversations. A speaker responded that usage trends are constantly evolving, and that Singaporean society was slow in harnessing social media platforms to engage in conversations and community relationship building. This was an area of interest for future research whereby mapping online discourses would allow researchers to track the evolution of patterns of societal connections online.

DISTINGUISHED LUNCH LECTURE

Legal Implications of Employing Social Media Analytics

Rebecca Weiner, Director of Intelligence Analysis, New York Police Department (NYPD)

Rebecca Weiner

Rebecca Weiner presented on the usage of social media by the New York Police Department (NYPD) to support investigations, and discussed the evolving legal architecture pertaining to law enforcement's use of social media to aid their work.

Weiner began her presentation by emphasising that terrorism continued to be a serious threat to national security. Prior to the Boston bombing, she revealed that some segments of the national security community in the US believed erroneously that the threat from terrorism had been significantly reduced. However, NYPD investigations had shown that terrorist plots were persistent, and in fact, many had targeted New York City (NYC).

She noted that the use of the internet and social media for terrorist-related activity had become a key issue in the US. For instance, Foreign Terrorist Organisations and their supporters were known to have used social media to reach out to English-speaking audiences as Ayman al-Zawahiri's English-subtitled sermons had underscored. Choosing potential targets, such as landmarks in NYC, were discussed extensively on online forums. There was also a concerted effort by jihadi groups to use the internet to recruit Westerners. A case in point was the recruitment of a US citizen, Samir Khan, who was initially part of Anwar Awlaki's "Internet mujahideen" and later became one of his actual fighters in Yemen. Furthermore, Jihadi groups were using social media as their main communication tool. Weiner also observed that jihadi groups were sophisticated and employed various

identity-concealment measures to avoid detection. These included operating multiple and semi-anonymous accounts across various social media platforms as well as employing aliases and proxy IP addresses. In light of this, the NYPD had established a specialised unit that was tasked with: (a) supporting investigations; (b) carrying out authorised investigations; (c) issuing legal requests; and (d) providing training.

Weiner observed that while social media platforms had begun to incorporate search functions (e.g. Facebook's Graph Search), it did not simplify investigations. Users were still largely anonymous on social media platforms, and as such, investigators had to rely on service providers to provide information to help identify individuals. She discussed the multi-stage process of obtaining information from service providers that have both administrative and legal dimensions. She also identified several difficulties related to obtaining social media data from service providers such as the geographical location of the company.

Weiner argued that in many cases, individuals who espouse extremist views online had a likelihood of engaging in violent activities in the physical world. She cited the examples of Rezwan Ferdaus, who was found guilty of a plot to attack the Pentagon with a remote-controlled aircraft packed with explosives; Quafi Nafeez, who was charged with attempting to detonate 1000 pounds of explosives in a car bomb in Manhattan; as well as Justin Keliebe, a Long Island resident who pleaded guilty to providing material support to an Al-Qaeda affiliate. These individuals had attracted the NYPD's attention with their extremist rhetoric online, and subsequent investigations had revealed their intentions.

With regard to the challenges pertaining to the legal architecture *vis-a-vis* online investigations, Weiner observed that the public was demanding more transparency on the part of the government while simultaneously advocating for more anonymity. Service providers have responded to the demands of their customers, and currently offered enhanced privacy protection on their platforms. Hence, retrieving personal data from such companies was not as easy as perceived.

An alternative strategy employed by some service providers, such as Facebook, was to encourage self-policing among users. Users could report suspicious online activities, abusive behaviour, the publishing of extremist content and other unsavoury activities.

Weiner then discussed how such privacy protection measures could adversely affect investigations. She cited the example of Twitter's policy of disclosure where it was obliged to notify users when a request for their information was made "unless prohibited by law from doing so" (i.e. prior notification). This process could delay investigations and impede them especially if the individual under investigation was put on alert.

In terms of policy-related challenges, Weiner observed that there was an increasing push for greater privacy protection and transparency in the West that would invariably affect how online investigations were carried out. Greater trust between law enforcement agencies and the public would have to be built if agencies were to remain operationally effective in this environment.

Discussion

A participant asked why terrorists were increasingly using social media despite the risks of being exposed. The speaker opined that this willingness to be open with their views/activities online was due in part to the general belief in the anonymity of the internet. Furthermore, some individuals took pride in their involvement in the jihadist cause, and wanted to declare it openly.

Another participant wanted to discuss the issue of transparency and privacy as it relates to investigations on social media more extensively. The speaker acknowledged that while there were legitimate concerns about transparency, privacy protection and accountability, a balance had to be struck with genuine security concerns and operational needs. She argued that law enforcement had taken increasing steps to protect the public's civil liberties than had been publicised. She added that investigations into an individual's actions were often targeted in order not to adversely affect the civil liberties of others. Law enforcement in the US, the speaker argued, faced many legal, administrative and constitutional constraints that prevented abuse.

SOCIAL MEDIA ANALYSIS – KEY ISSUES

Digital Maturity Psycho-Social Maturity and Implications

Majeed Khader, Director, Behavioural Science Unit, Home Team Academy (HTA), Singapore

Majeed Khader

Majeed Khader began his presentation by discussing the concept of digital lifespans. He argued that "tech" skills were increasingly replacing "life" skills with the advent of the digital age. Citing several quantitative studies, Khader argued that children were now more technically savvy then they had been in the past. They were able to use computers, smartphone applications and even surf the internet competently. Many online "playgrounds" where children could establish social networks (e.g. webkinz and club penguin) have emerged as a consequence. Expectedly, the risks associated with this trend such as children being exposed to aggressive and/or inappropriate behaviour online have increased as well. Khader also argued that teenagers were at an even greater risk of being exposed to as well as perpetrating unacceptable behaviour online. Of significant concern was that they were not aware of the long-term implications and/or consequences of such behaviour on themselves or their "victims/targets". Privacy issues and location disclosure through geo-tagging were cases in point. Khader argued that that the development of digital maturity in an individual could not be achieved without the development of his/her physical, behavioural, cognitive, social and emotional maturity. It was therefore important to focus on developing all these different aspects of maturity especially in the young.

Khader then discussed several key features of the internet and social media that significantly impacted the psychology of individuals, and in turn, digital and non-digital maturity development. With regards to the internet, it: (a) transcended geography, and enabled individuals with shared interests to come together; (b) facilitated the multiplication of social links, which enabled users to establish and juggle many relationships simultaneously; (c) enabled synchronous communication; (d) was recordable, which enabled psychological re-experiencing; and (e) promoted dis-inhibition due in part to a false sense of anonymity, which encouraged brazenness and misbehaviour in some individuals. He further added that virtual communities were highly significant for the following reasons: (a) interactional aspects of the internet were highly addictive; (b) provides emotional rewards of belonging; (c) "fictive kin" replaces lost ties to family and community; (d) provides sense of meaning and purpose; (e) reduces influence of mainstream beliefs and ideas; (e) allows for "unobtrusive lurking"; and (f) fragments "real communities". In relation to social media, content was: (a) persistent – expressions made online were easily archived; (b) replicable – information could be easily duplicated; (c) searchable; and (d) easily doctored. The three main factors affecting the dynamics of online networked communities were: (a) invisible audiences; (b) the absence of context; and (c) the blurring of public and private. Some examples cited included cyber bullying, internet love and sex scams. In light of such dynamics, it was necessary to develop virtual immune systems and cyber resilience though educating both children and adults on such pitfalls.

Khader proposed several initiatives to address these concerns including: (a) the development of virtual immune systems and cyber resilience through: (i) fostering children's "virtual immune systems"; (ii) nurturing children online and offline; (iii) monitoring internet addiction; and (iv) paying attention to older children; (b) the need to study more closely the link between internet deviance, cybercrime and human interface; (c) fine-tuning legalisation and law enforcement policies for the digital age; and (d) developing new ways to leverage the internet for positive outcomes.

Managing Risks of Social Media in the SAF

Sam Lee Hsiang Wei, Republic of Singapore Air Force

Lee Siang Wei

Lee Siang Wei began his presentation by defining social media as a type of online media that expedites conversations through the creation and exchange of user-generated content that was targeted. This unprecedented level of interaction made social media highly appealing and attractive to many around the world. With the speed at which social media continued to grow and multiply, Lee believed that the Singapore Armed Forces (SAF) could not afford to ignore the inherent risks. These could easily be exploited both within and outside of the military context. It was therefore crucial for the SAF to adapt its social media policy to prevailing trends in the social media landscape as they emerge. By ensuring that several key elements were achieved, social media would become a more manageable medium without compromising information and operational security in the armed forces.

Lee said that the SAF recognised that there were effectively two sides to a soldier: the professional and the personal. The professional face of the soldier was one that was always operationally-ready in his/her line of work, in the soldier's personal capacity, he/she was a brother/sister, friend, son/daughter. Lee believed that there was a need to be aware of the dual roles of the soldier when formulating policies on social media.

While the SAF recognised that it was unable to prevent its personnel from using social media, it was aware of the risks for the organisation as well. These risks were broadly divided into *user-related* and *system-related* categories. Risks in the former category related to direct disclosure when users inadvertently shared critical information to the public. Lee cited the example of how a raid on a Palestinian village in March 2010 had to be cancelled after an Israeli soldier disclosed information about the operation on Facebook. User-related risks also included the accidental revelation of locations in light of the rise of geo-location social media applications.

In terms of system-related risks, these occurred as a result of user anonymity online. Lee observed that the ease of setting up false social media accounts could easily mislead users into providing sensitive information to unauthorised individuals. Lee cited the "Robin Sage" experiment in 2009 as a case in point. A fictitious cyber security analyst, Robin Sage, was able to obtain invitation to conferences as well as solicit potentially sensitive information from several security professionals.

Another system-related risk is one by design. Lee observed that the default settings of many social media platforms tacitly compel users to make more personal information public. For instance, the privacy policies of Facebook have evolved such that more user information is now shared than before. Lee noted that most users were not aware of the changes in these policies, and few actually read the terms of service carefully.

System-related risks could also come from information aggregation. Piecing together seemingly unimportant information on social media can in fact reveal a lot. For instance, mapping the network of the 9/11 suspects was conducted by this process of information aggregation. The contemporary social media landscape yields far more information than before, and as a result, can be used effectively for information-gathering.

Lee concluded by suggesting that organisations review their social media policies regularly and to educate staff on proper usage in order to minimise the risks associated with social media.

Discussion

A participant asked how policy makers should respond to online protests and activism. A speaker argued that while there were arguments for criminalising such actions, other alternatives were available, and could be used instead. These included self-policing and encouraging netizens to establish and adhere to normative behaviours.

A participant inquired as to how the community could help the victims of online abuse and whether the community could play an autonomous role in addressing cyber wellness. A speaker noted that in the social media discourse little has been mentioned about the role of the community at large. There have been instances where local groups have come together in support of the victim(s). The speaker added that to foster individual resiliency against cyber abuse, it was crucial to draw lessons from resilience psychology and teach the victims how to move forward. In relation to cyber wellness, the speaker cited an example where some individuals established an online group prior to moving in to their new flats to establish contact with each other and to discuss related issues. He noted that it was possible to determine normative behaviour online, but this was highly dependent upon the catalysts or influencers in the community.

CASE STUDIES

The Role of Social Media in the Response to the Marathon Attacks

John Daley, Chief Technology Officer and Deputy Superintendent, Boston Police Department

John Daley

John Daley highlighted the importance of police departments participating in online conversations, particularly during a crisis. This serves not only as a way for the police to provide timely and accurate information to the general public, but also opens channels for the authorities to receive critical information from the public during a crisis.

Daley first discussed the period before the Boston Marathon Bombing when the Boston Police Department (BPD) was compelled to increase its online media capabilities due in part to its conflict with two newspapers. To reduce its reliance on mainstream media, a website – BPDNews.com – was established to communicate directly with the public. Through the website, the BPD was able to provide timely information to the public and tell its side of the story, which enabled it to build public confidence. In 2008, the BPD also established a Twitter account (@BostonPolice), which was used to announce police activities such as street closures. The BPD also established a hashtag on Twitter (#tweetfromthebeat), which allowed the community to file complaints or comments about law and order issues. This interaction between the BPD and the local community, Daley opined, demonstrated that

the department was an accepted and respected member of the community.

The established channels of communication online as well as the strong relationship between the BPD and the community were instrumental in the Boston Marathon bombing of 15 April 2013. In the period immediately following the attack, police officers were not only tending to victims, protecting the crime scene and trying to prevent further attacks, they were also active on social media directing people how to respond, as well as having BPD online posts translated into different languages so as to make the information accessible to the entire community. The BPD also used their presence on social media to seek information (particularly videos and photos) from the public that would assist in investigations. The BPD and the Federal Bureau of Investigation (FBI) were subsequently inundated with the voluminous information they received.

Daley went on to discuss the media debacle in the aftermath of the bombing, whereby the major media outlets had disseminated erroneous information to the public. For instance, the New York Post incorrectly identified an individual as being the Boston bomber, and Fox News had prematurely announced that the bomber had been arrested. The BPD intervened, and subsequently became the authoritative source of information, which helped to ensure the accuracy of information that was being disseminated.

Daley concluded by sharing the BPD's guiding principles of public engagement on social media. These were: (a) integrate social media into everyday business – from routine to critical; (b) utilise social media for dialogue as well as to broadcast information; (c) expand communication scope beyond simply providing public information; and (d) listen to what people are saying, and respond accordingly, as opposed to simply monitoring conversations.

Social Media and Opensource Intelligence: Lessons from the London Olympics
Daniel Piece, Head of the London Metropolitan Police All Source Hub

Daniel Pierce

Daniel Pierce discussed his experience as Head of the London Metropolitan Police All Source Hub during the London Olympics in 2012. He said that the policing and securitisation of the event was a gargantuan task that involved eight years of planning and considerable finances. He revealed that intelligence gathering through social media platforms was extremely challenging as well. It involved 24-hour monitoring and extensive filtering of Facebook and Twitter posts, which ultimately produced 31 million security-relevant posts as well as 2562 intelligence reports.

Pierce noted that one of the key lessons from the London Olympics was not to assume that individuals had a firm grasp of social media, and in particular, senior officials and politicians. He observed that initially, social media was not given adequate attention or resources due to a general lack of understanding of how the platform functioned and the useful information that could be mined from it.

Another lesson learnt was that social media could provide a wealth of intelligence to authorities. He observed that individuals generally felt the need to share much of their personal information on social media. This meant that by carefully analysing the online footprints left by suspects as well as their family and/or friends, useful intelligence could be gathered to help in investigations.

Pierce then discussed some of the main operational challenges of using social media for intelligence gathering at the London Olympics. These included: (a) the need to collect and analyse vast amounts of data; and (b) the need for increased funding and staff to so. Moreover, he observed that as there was ambiguity about the legality of social media intelligence gathering, issues concerning privacy and the dissemination of intentional misinformation would invariably arise.

Pierce observed that while there were several analytics software available, it was important to select tools that were of relevance. Analytics tools should, at the very least, be able to conduct horizon scanning, sentiment analysis, bot spotting (such as analysing Twitter for low tweets, follower ratios, user reputation, etc.), analytical trending, linguistic analysis and geo-tagging analysis.

Pierce concluded his presentation by arguing that the private sector and academia should continue to lay the groundwork for educating individuals, especially senior policy makers, in the use and value of social media. He also noted that social media must be integrated throughout policing activities. With regard to online intelligence gathering, he suggested that efforts should be focussed on analysing the digital footprints of suspects as well as their friends and families. This could provide vital clues on potential terrorist cells, protest events and emerging protest groups.

He emphasised the necessity for law enforcement agencies to enhance their capabilities in terms of: (a) picking up on suspicious activities before they escalate; (b) efficiently reviewing the sentiments of the public from their social media activity; (c) effectively reviewing geo-tagged tweets; (d) identifying how influential a suspect is in his/her social network; and (e) providing timely information to senior officers and decision makers. He also suggested that law enforcement agencies actively engage with the general public on and off line, and especially during a crisis, and also to use social media experts and subject matter experts to better understand the nuances of social media, such as the different demographic preferences for various social media platforms.

CERA's use of Social Media Analytics for Disaster/Emergency Operations

Mike Shatford, Deputy Chief Executive, Communications, Canterbury Earthquake Recovery Authority (CERA)

Mike Shatford

Mike Shatford began his presentation by first discussing the impact of the earthquakes in New Zealand that occurred in 2010 and 2011. A 7.1 magnitude earthquake struck the South Island of New Zealand on 4 September 2010. There were more than 13,000 aftershocks following that, with the worst occurring on 22 February 2011. 185 lives were lost and 11,432 people injured as a result. There was widespread damage to water, sewerage, power and telecommunications. This was uncharted territory for people, communities, business, councils and the government.

He then went on to describe the work of the Canterbury Earthquake Recovery Authority (CERA). CERA was established in the wake of the disaster to lead and coordinate the ongoing recovery effort. Its role includes: (a) providing leadership and coordination for the ongoing recovery effort; (b) focusing on business recovery, restoring local communities and making sure the right structures are in place for rebuilding; (c) enabling an effective and timely rebuilding; (d) working closely with Christchurch City Council, Selwyn District Council, Waimakariri District Council and Environment Canterbury and engaging with local communities of greater Christchurch, including Ngāi Tahu, the private sector and the business sector; and (e) keeping people and communities informed.

Next he talked about CERA's communication strategy, which was premised on active engagement with the community throughout its recovery framework. This framework comprised of: (a) responding; (b) rebuilding; and (c) recovery. With regard to *response*, there was no structure to support and indeed no plan to use social

media as a communication medium at the outset. A traditional one-way top-down communication system was in place, and this prevented a two-way conversation between the government agencies and the public from occurring. This meant that there was no way to understand the mood of the community and no effective processes to receive and answer queries. CERA therefore began using Facebook and Twitter for the first several months solely to publicise CERA and Ministerial press releases, announce Central Business District (CBD) cordon changes, and repost information from the Canterbury Earthquake website and Christchurch City Council.

In relation to *rebuilding*, CERA was both reactive and proactive, and tried to build up the confidence of the general public, as well as encourage them to participate in the recovery efforts. A case in point was the "Share an Idea" campaign, which was initiated to gather input from the public to help develop a recovery plan for the central city. The inherent challenge was how to get Christchurch people to express their views quickly, while people were still suffering. The campaign was designed as a city-wide conversation, and used social media as a key way to communicate and consult. Over time the campaign's focus changed from eliciting general ideas from the public to eliciting specific ideas on emerging themes and issues. Other channels of communication were also used in conjunction with social media to achieve the maximum reach.

With regard to *recovery*, a long-term and proactive approach was used. Furthermore, it focused on the co-creation of solutions, and was largely community-driven. One example of how this was operationalized was the 'Youth Wellbeing Survey'. This was part of a reporting and monitoring programme that tracked the progress of Canterbury's recovery over time. Residents of the greater Christchurch area who were between 12 and 24 years old were given opportunities to voice their opinions on rebuilding the city online.

Shatford concluded by discussing several takeaways with regard to the use of social media during disaster relief operations He urged government agencies to develop a coordinated crisis plan that involved all departments. He suggested that alternative communication channels had to be established in the event of a power failure during a crisis. Finally, he maintained that creating trust between the government and the public was paramount during

a crisis, and this could be accomplished by: (a) having credible spokespersons; and (b) providing information that is reliable, verifiable and immediate through a range of channels.

Discussion

A participant was interested to know if social media had contributed to the spread of violence during the 2011 riots in the United Kingdom. A speaker said that while social media did play a considerable role in the 2011 riots, the media had exaggerated the extent of its utility. He revealed that shutting down the internet in the affected areas had been considered, but was subsequently abandoned in light of the expected backlash.

Another participant inquired about the specific measures taken by the New Zealand authorities after the Canterbury earthquake to restore public trust. A speaker responded by highlighting that CERA was headed by a well-known member of the local community, and as such, there was a significant level of trust pre-existing. Furthermore, two-way communication strategies and active collaboration between CERA, community leaders and local stakeholders also helped.

MORNING LECTURE

Social Media and The Arab Spring

Nasser Wedaddy, Outreach Director, American Islamic Congress (AIC)

Nasser Weddady

Given the long history of government repression of media in Arab countries, the unprecedented flow of information brought about by the internet played a transformative role in Middle East politics. While online platforms such as blogs and social media have facilitated free exchange of ideas that later unleashed widespread social discontent, it is the human networks behind them that constitute the actual driving force of the Arab Spring uprisings. The engine behind social media, that is the human networks and the strategies they employed were the focus of **Nasser Weddady's** lecture.

Weddady argued that in order to get a clear picture on the transformative role of the internet in the Arab world, it was important to understand the history of political repression and media censorship in many Arab countries. Egyptian and Mauritanian governments, for instance, had for many decades imposed strict censorship on mass media and book publications, which created a tremendous hunger for information. In this context, the internet was a significant game-changer as it allowed people to access information from local and foreign media freely and instantaneously. With the introduction of social media, people were able to bypass the state messaging boards, which did not allow for the free and frank exchange of ideas and did not promote individuality or self-expression.

While much had been discussed about blogs and social media in Arab political transformation, there remained

a missing part of the story: the transnational network of political activists and their strategy. The activist network played a central role in translating online activism into political mobilisation in the real world. One of the important figures in this network was Ali Abdul Imam from Bahrain, who founded the Bahrain Online website in 1998. By 2002, his forum had become the primary gathering place online for Bahraini opposition. This forum subsequently contributed to the mobilisation of 250 000 protestors to rally on the streets. As such, Iman was the first activist to prove that online activism could have a real world impact. His success was followed by other activists in the network, including Wael Abbas, one of the most seminal Egyptian bloggers at the outset of the Arab Spring.

Weddady explained that the network activists generally employ two broad communication strategies for political mobilisation. The first strategy is called cross-posting for advocacy (CPA). CPA weaves various online platforms together to maximise the campaign outreach. To be effective, the information disseminated through CPA needs to be both rich and condensed. As Weddady put it, CPA uses "twitter language" in order to provide the maximum amount of data with the minimum amount of clicks. CPA-based campaigns have not only resulted in mass mobilisation but also real changes. A case in point is the "free x" campaign series, which successfully pressured several governments to free political prisoners.

Besides direct campaigning and advocacy, activists also use mass media to support their efforts. Their media communication strategy has two components. Firstly, they try to understand the nature of different media – local and Western – and present the information in accordance with established criteria to gain acceptance. Secondly, the network also helps connect local activists to international journalists. The overall aim of this strategy is to shape the global media narrative on the uprising, thus breaking the government monopoly of the creation of political narrative.

In conclusion, Weddady re-emphasised the significance of the human network and effective communication strategies in bringing online political activism to real

life revolution. At the same time, he was mindful of the flipside of online platforms as they could be used by authoritarian governments as a barometer of social discontent and potential unrest. Hence, those intending to use social media for political purposes need to be mindful of its potential to be a double-edged sword.

Discussion

A participant asked about the attributes that made someone influential in the realm of online activism. The speaker mentioned two factors in response: (a) an individual's ability to add value to the conversation i.e. through developing effective communication strategies or connecting activists to journalists; and (b) an individual's reputation and level of influence in the real world.

Another participant raised the issue of political instability in the aftermath of the Arab Spring, and asked whether the Arab network of activists could also contribute to stabilising efforts. The speaker responded that the network was already undertaking efforts towards stability

creation in at least three ways. First was through the promotion of democratic ideals. Secondly, the network's tactic of strategic disruption remained useful to disrupt political structures that contribute to existing instability. Thirdly, and perhaps most importantly, instilling a sense of individual responsibility and social entrepreneurship in the minds of the people, so they could rely on themselves rather than the government to tackle various social problems.

A participant asked about the significance of smartphones for mass mobilisation during the uprising, and whether it had prompted government restrictions of smartphone use. Weddady confirmed that smartphone and broadband penetration throughout the Arab world was very important mainly because it enables video transmission. This constituted the main medium of information diffusion in a region where the literacy rate was still low. Countries have not restricted smartphone use but have slowed down internet speeds to disrupt connections during instances of social unrest.

PANEL 5:
EFFORTS TO IMPROVE DIGITAL MEDIA LITERACY

Singapore's Media Literacy Council – 1 Year On
Lai Lei Khim, Executive Director, Media Literacy Council Singapore

Lai Lei Khim

Lai Lei Khim began her presentation with a brief overview of the internet landscape in Singapore. She pointed out that internet usage is highly skewed towards the younger age groups, mainly those under 35. She opined that cyberspace had become the new playground, and as a result, many activities that were traditionally carried out in the real world were now being replaced with activities online. For example, Google had replaced libraries as a knowledge repository, online learning had replaced traditional classroom learning, and more individuals are reading newspapers, watching TV and communicating online. But at the same time, the advantages of the internet have been marred by its negative aspects such as cyber bullying. Lai argued that the openness, speed and permanence of the internet were increasing the good, the bad as well as the ugly side of human nature.

Lai then gave a brief overview of Singapore's Media Literacy Council (MLC), and its primary roles. She also discussed MLC's desired public education outcomes, which focussed on fostering discerning Singaporeans who would be able to evaluate media content effectively, and be able to use, create and share content safely and responsibly. She explained that these objectives were to be accomplished through joint partnerships with the private sector, community and the government.

Lai then discussed the four-pronged outreach strategy that MLC use to achieve their goals, which includes: (a) national public education through campaigns and media

opportunities; (b) outreach programs and events; (c) research, which includes creation of new conversations and thought-leadership; and (d) resource development, such as handbooks, training kits, apps and videos. She explained that the main target audience of MLC's outreach was young children, teenagers as well as young working adults.

Lai also elaborated on the aforementioned activities, as well as the partnerships the MLC had built. Some of the MLC's public awareness initiatives included Safer Internet Day, which was organised this year for the first time. Communication literacy seminars were also carried out where experts from around the world were invited to share their experiences. Regarding the youth programs, she observed that peer-to-peer learning had proven to be effective and engaging way of learning among young people. Therefore, the MLC has started to promote a Media Smart Club, which involves the most active students who are trained and educated in media literacy issues and who are subsequently involved in running events throughout the year, to share their knowledge with their peers.

Enhancing Access and Use of Media and ICTs through Media and Information Literacy
Alton Grizzle, Programme Specialist, Communication and Information Sector (CI), UNESCO

Alton Grizzle

In his presentation on UNESCO's work on Media and Information Literacy (MIL) **Alton Grizzle** suggested that four complementary elements were needed to make MIL a mass, engaging, civic education movement. These included: (a) common curriculum for media literacy;

(b) effective policies and strategies; (c) assessment framework; and (d) networking and global partnerships.

He pointed out that in light of both the risks and opportunities on the internet, it was crucial to develop information and media literacy skills in citizens, especially the young. He argued that media literacy was traditionally taught as part of informal education but as individuals now spend more time in the virtual world, it was necessary for media and information literacy to become part of formal education and made available to all students. Grizzle observed that it was commonly argued that the risks on the internet should be mitigated by developing strategies for the protection of users. However, he opined that it was more important to develop preventive strategies that focus on the empowerment of individuals, which would enable them to tackle online security threats in a mature and effective way. He argued that this was where media and information literacy was most beneficial. In his opinion, technologies evolve constantly, and therefore, fool-proof protection was simply impossible. Hence, it was more prudent to focus on individual empowerment instead.

He explained that UNESCO has accepted the fact that there was confusion over the term Media and Information Literacy, and rather than attempting to join the debate or provide a clear definition of the concept, the organisation had chosen instead to focus on the key learning outcomes. UNESCO regards both information and media literacy skills as equally important. He discussed the organisation's Global Media and Information Literacy curriculum, which was developed as a holistic approach to the different types of literacies. This curriculum has been translated into 15 different languages, and at present, UNESCO was working with different countries to adapt and adopt this curriculum into their respective formal education systems.

In closing, he emphasised that MIL was about people and about empowering citizens with skills to actively participate in development, good governance, peace, intercultural dialogue and democracy.

Facing Online Hate: A Canadian Approach
Matthew Johnson, Director of Education, MediaSmarts, Canada

Matthew Johnson

In discussing the Canadian approach to facing hate speech online, **Matthew Johnson** first explained how MediaSmarts, a not-for-profit charitable organisation for digital and media literacy, understood online hate. He then explained why MediaSmarts had chosen to focus on youth as the main target group. Lastly, he discussed several strategies that could be employed to deal with offensive material online.

Johnson explained that online hate was not understood as an emotion, but rather as a mindset or a point of view where people defined themselves in opposition to another group. He clarified that much of the hate material on the internet produced by hate groups and/or individuals did not meet the legal definition of hate speech. MediaSmarts' definition of online hate was much broader than the legal one, and included all forms of online communication that denigrated or promoted hatred of a particular group. This included a wide range of manifestations of hate – from White supremacists to religious terrorists to those promoting ethnic hatred towards groups such as Mexicans, Koreans and Roma. He argued that the existing laws in Canada were only effective in dealing with the most clear-cut examples of hate speech, whereas the rest of hate and discrimination material online was effectively not regulated.

He explained that MediaSmarts' decision to focus primarily on young people was due in part to the fact that youth (primarily males between the ages of twelve and seventeen) were found to be the main group responsible for hate crime offences offline. He further explained that in the online realm, youth do not have to encounter

overt hate speech to be exposed to hate. "Cultures of hatred" existed openly, and could easily radicalise young people. Some gaming cultures for instance, promoted racism, misogyny and other prejudices as normative behaviour. Cloaked sites were yet another pathway to youth radicalisation. Here, such sites present themselves as being neutral and educational, but communicate a subtle message of hatred.

Johnson also elaborated on the strategies that were useful in countering online hate speech. He argued that a comprehensive anti-hate program that encompasses all of the skills young people need when they encounter online hate was indispensable. He pointed out that it was necessary that youth were equipped with skills to recognise the techniques hate groups use to make their arguments, manipulate events and information, and promote their ideologies indirectly. Furthermore, he argued that it was important to encourage empathy development in young people so they can recognise and respond to hate when they see it. One such program used by MediaSmarts for fighting cyber bulling was the *Roots of Empathy* program, but could also be used to combat online hate. He also opined that incarcerating youth for hate crimes was an ineffective strategy as many Neo-Nazi organisations, such as the Aryan Brotherhood, use prisons to recruit.

Lastly, he noted that MediaSmarts had developed a guide on *Responding to Online Hate*, which was designed to provide useful tools for parents, educators and law enforcement, with which they could use to engage young people.

Discussion

A participant was interested to know if parents are taught how to activate filters in order that they can prevent their children from accessing questionable websites. A speaker answered that usually a more holistic approach in educating parents was employed because often, it was not so much about the technical skills of the parents but about their parenting skills. The speaker pointed out that a lot of parents know about filters but they do not think it is very useful so they do not activate them. Accordingly, parents are taught how they can use tools to monitor their children's behaviour online.

Another participant was interested to know how and what were the best practices and techniques to respond to hate speech online. A speaker answered that primarily, it involved teaching young people how to recognise dishonesty, how to be critical and discerning about information and distinguish between legitimate debate and hate mongering.

WORKSHOP AGENDA

Thursday, 31 October 2013
Social Media Analysis

0800 – 0900hrs   **Registration**
Venue:
Vanda Ballroom Foyer, Level 5

0900 – 0915hrs   **RSIS Corporate Video + Welcome
Remarks** by *Kumar Ramakrishna,*
*Head, Centre of Excellence for National
Security (CENS), RSIS, NTU*
Venue:
Vanda Ballroom, Level 5

Attire:
Smart Casual
(Long-Sleeved shirt without tie)

0915 – 1045hrs   **Panel 1: Social Media Analytics:
Social Media Analytics in
Investigation and Analysis**
Venue:
Vanda Ballroom, Level 5

Chairperson:
Kumar Ramakrishna, *Head, Centre of
Excellence for National Security
(CENS), RSIS, NTU*

Speakers:
**Defending the Realm using Social
Media Analytics** by *Alan Jenkinson,*
*Director of Strategic Business - Home
and Foreign Affairs at Hewlett-Packard*

**The Facebook Effect: A Law
Enforcement Perspective** by
*Nick O'Brien, Associate Professor
Counter Terrorism and Head of
School, Australian Graduate School of
Policing and Security, Charles Sturt
University*

**Using Social Media Analytics in
Investigation and Analysis – Current
Issues and Future Trends** *by Stephen
Tracy, Insight & Analytics (I&A) Lead for
APAC, Waggener Edstrom*

Q & A

1045 – 1100hrs   **Tea Break**
Venue:
Vanda Ballroom Foyer, Level 5

1100 – 1245hrs   **Panel 2: Social Media Analytics:
New and Emerging Technologies**
Venue:
Vanda Ballroom, Level 5

Chairperson:
*Caitríona H. Heinl, Research Fellow,
Centre of Excellence for
National Security (CENS), RSIS, NTU*

Speakers:
**[SKYPE Presentation] GDELT:
Realtime Automated Global
Behavior and Beliefs Mapping,
Modeling, and Forecasting Using
Hundreds of Millions of Events**
*by Kalev H. Leetaru, Yahoo! Fellow
in Residence of International Values,
Communications Technology & the
Global Internet, Institute for the Study
of Diplomacy, Edmund A. Walsh School
of Foreign Service, Georgetown
University*

**Making Sense of Social Media:
Who, What, How** by *Carol Soon,
Research Fellow, Institute of Policy
Studies, NUS, with contributions from
Marc Smith, Chief Social Scientist,
Connected Action Consulting Group*

Social Hacking and Cognitive Security *by **Rand Waltzman**, Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)*

Social Analytics using Twitter Data *by **Lim Ee Peng**, Professor of Information Systems, Director, Living Analytics Research Centre, Singapore Management University (SMU)*

Q & A

1245 – 1320hrs **Distinguished Lunch Lecture**
Venue:
Vanda Ballroom, Level 5

Chairperson:
Damien D. Cheong, *Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speaker :
Legal Implications of Employing Social Media Analytics *by **Rebecca Weiner**, Director of Intelligence Analysis, New York Police Department (NYPD)*

Q&A

1320 – 1430hrs **Lunch**
Venue:
Pool Garden, Level 5

1430 – 1530hrs **Panel 3: Social Media Analysis – Key Issues**
Venue:
Vanda Ballroom, Level 5

Chairperson:
Damien D. Cheong, *Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers:
Psychological Considerations for Digital Maturity: What are the Security Challenges and Implications? *by **Majeed Khader**, Director, Behavioural Science Unit, Home Team Academy (HTA)*

Managing the Risks of Social Media in the SAF *by **Sam Lee Hsiang Wei**, Republic of Singapore Air Force*

Q & A

1530 – 1550hrs **Tea Break**
Venue:
Vanda Ballroom Foyer, Level 5

1550 – 1720hrs **Panel 4: Case Studies**
Venue:
Vanda Ballroom, Level 5

Chairperson:
Norman Vasu, *Deputy Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers:
The Role of Social Media in the Response to the Marathon Attacks *by **John Daley**, Chief Technology Officer and Deputy Superintendent, Boston Police Department*

Social Media Intelligence – Lessons learnt *by **Daniel Pearce**, Head of Analysis, Open Source and Social Media, Metropolitan Police Service*

CERA's use of Social Media Analytics for Disaster/Emergency Operations *by **Mike Shatford**, Deputy Chief Executive, Communications, Canterbury Earthquake Recovery Authority (CERA)*

Q & A

| 1720hrs | **End of Day 1** |
| 1830 – 2100hrs | **Workshop Dinner (by Invitation Only)** |

Friday, 1 November 2013
Digital Maturity

0800 – 0900hrs	**Registration**
	Venue:
	Marina Mandarin Ballroom Foyer, Level 1

0900 – 1000hrs	**Morning Lecture**
	Venue:
	Marina Mandarin Ballroom, Level 1

Chairperson:
***Sulastri Osman**, Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers:
Social Media and The Arab Spring – Tweeting the Uprisings *by **Nasser Weddady**, Outreach Director, American Islamic Congress (AIC)*

1000 – 1030hrs	**Tea Break**
	Venue:
	Marina Mandarin Ballroom Foyer, Level 1

1030 – 1200hrs	**Panel 5: Efforts to Improve Digital Media Literacy**
	Venue:
	Marina Mandarin Ballroom, Level 1

Chairperson:
***Yolanda Chin**, Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers:
Singapore's Media Literacy Council – 1 Year On *by **Lai Lei Khim**, Executive Director, Media Literacy Council*

Enhancing Access and Use of Media and ICTs through Media and Information Literacy *by **Alton Grizzle**, Programme Specialist, Communication and Information Sector (CI), UNESCO*

Facing Online Hate: A Canadian Approach *by **Matthew Johnson**, Director of Education, MediaSmarts, Canada*

Q & Q

1200 – 1330hrs	**Lunch**
	Venue:
	Pool Garden, Level 5

1330 – 1630hrs	**Social Media Table Top Exercise**
	Venue:
	Marina Mandarin Ballroom, Level 1

1630 – 1645hrs	**Tea Break**
	Venue:
	Marina Mandarin Ballroom Foyer, Level 1

1645 – 1745hrs	**Debrief**
	Venue:
	Marina Mandarin Ballroom, Level 1

| 1745hrs | **End of Day 2** |

| 1830 - 2100hrs | **Closing Dinner (by Invitation Only)** |

LIST OF SPEAKERS AND CHAIRPERSONS

SPEAKERS

John Daley
Boston Police Headquarters
1 Schroeder Plaza
Boston, MA 02050
USA
Email: john.daley@pd.boston.gov

Alton Grizzle
Programme Specialist
UNESCO
7 place de Fontenoy
75352 Paris 07 SP
France
Email: a.grizzle@unesco.org

Alan Jenkinson
UK Communities & Government Sector Policing
and Sector Innovation Lead
HP Enterprise Services Ltd
Cain Road,
Bracknell, Berkshire, RG12 1HN
UK
Email: alan.jenkinson@hp.com

Matthew Johnson
Director of Education
MediaSmarts
950 Gladstone Avenue, Suite 120
Ottawa, Ontario
Canada
K1Y 3E6
Email: MJohnson@mediasmarts.ca

Majeed Khader
Director
Behavioural Sciences Unit
Home Team Academy
501 Old Choa Chu Kang Road
Singapore 698928
Email: khader_majeed@mha.gov.sg

Lai Lei Khim
Executive Director
Media Literacy Council
3 Fusionopolis Way #16-22 Symbiosis
Singapore 138633
Email: lai_lei_khim@mda.gov.sg

Sam Lee Hsiang Wei
Pilot
Republic of Singapore Air Force
315 Sembawang Road
Singapore 757755
Email: samlee85@gmail.com

Kalev H. Leetaru
2013-2014 Yahoo! Fellow
Residence of International Values
Communications Technology & the Global Internet
Institute for the Study of Diplomacy
Edmund A. Walsh School of Foreign Service
ICC 301, Georgetown University
Washington D.C. 20057
Email: kalev.leetaru5@gmail.com

Lim Ee Peng
Director
Living Analytics Research Centre
School of Information Systems
Singapore Management University
80 Stamford Road
Singapore 178902
Email: eplim@smu.edu.sg

Nick O'Brien
Associate Professor Counter Terrorism
and Head of School
Australian Graduate School of Policing
Charles Sturt University
10 - 12 Brisbane Avenue
Barton ACT 2604
Australia
Email: nobrien@csu.edu.au

Daniel Pearce
Head of Analysis, Open Source and Social Media
Metropolitan Police Service
10 Victoria Street
London
UK
Email: Daniel.Pearce@npoiu.pnn.police.uk

Mike Shatford
Deputy Chief Executive, Communications
Canterbury Earthquake Recovery Authority
62 Worcester Boulevard
Christchurch
New Zealand
Email: mike.shatford@cera.govt.nz

Carol Soon
Research Fellow
Institute of Policy Studies
Lee Kuan Yew School of Public Policy
National University of Singapore
1C Cluny Road House 5
Singapore 259599
Email: carol.soon@nus.edu.sg

Stephen Tracy
Asia-Pacific Insight & Analytics Lead
APAC, Waggener Edstrom
3 Pickering Street, #02-50 Nankin Row
China Square Central
Singapore 048660
Email: stracy@waggeneredstrom.com

Rand Waltzman
Program Manager
Information Innovation Office
Defense Advanced Research Projects Agency
675 North Randolph Street
Arlington, VA 22203-2114
USA
Email: rand.waltzman@darpa.mil

Nasser Weddady
Civil Rights Outreach Director
American Islamic Congress
38 Newbury Street, Suite 702
Boston, MA 02116
USA
Email: weddady@aicongress.org

Rebecca Weiner
Director of Intelligence Analysis
Intelligence Division
New York City Police Department
1 Police Plaza
New York, N.Y. 10038
USA

CHAIRPERSONS

Damien D. Cheong
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: isdcheong@ntu.edu.sg

Yolanda Chin
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: istlchin@ntu.edu.sg

Caitríona H. Heinl
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: ischeinl@ntu.edu.sg

Sulastri Osman
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: issulastri@ntu.edu.sg

Norman Vasu
Deputy Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: isnvasu@ntu.edu.sg

Kumar Ramakrishna
Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: iskumar@ntu.edu.sg

LIST OF PARTICIPANTS

Umar Bin Abdul Ngalim
SSO Social Media
Singapore Civil Defence Force
91 Ubi Avenue 4
Singapore 408827
Email: umar_abd_ngalim@scdf.gov.sg

Charmaine Ang
Senior Consultant
Ministry of Home Affairs
28 Irrawaddy Rd
Tower M, Level 12
Singapore 329560
Email: charmaine_ang@mha.gov.sg

Jansen Ang
Deputy Director
Ministry of Home Affairs
501 Old Choa Chu Kang Road
Singapore 698928
Email: jansen_Ang@spf.gov.sg

Rozita Binti Anwar
Senior Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawady Road
Singapore 329560
Email: Rozita_ANWAR@spf.gov.sg

Vidia Arianti
Associate Research Fellow
S. Rajaratnam School of International Studies
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: isvidia@ntu.edu.sg

Nur Azhar Ayob
Senior Assistant Director
Ministry of Home Affairs
New Phoenix Park
28 Irrawady Road
Singapore 329560
Email: nur_azhar_ayob@mha.gov.sg

Devrajan Bala
Deputy Director
National Security Coordination Secretariat
55 Newton Road
#15-00, Revenue House
Singapore 307987
Email: devrajan_bala@nscs.gov.sg

Bay Chin Loo
Senior IT Consultant
Ministry of National Development
5 Maxwell Road
#19-00, Tower Block
MND Complex
Singapore 069110
Email: Bay_Chin_Loo@mnd.gov.sg

John Callahan
Associate Director
Office of Naval Research Global
86 Blenheim Crescent
Ruislip, HA4 7HB
UK
Email: john.r.callahan.civ@mail.mil

Sarah Campbell
Manager, Strategic Policy Analysis / SID-IC
Defense Advanced Research Projects Agency
675 North Randolph Street
Arlington VA 22203
USA
Email: sarah.campbell.ctr@darpa.mil

Grace Chen
Executive
Ministry of Communications and Information
140 Hill Street
4th Storey
Singapore 179369
Email: grace_chen@mci.gov.sg

Belinda Cheng
Senior Executive
Ministry of Home Affairs
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: belinda_cheng@mha.gov.sg

Chew Lock Pin
Director, RAHS Programme Office
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: Chew_Lock_Pin@nscs.gov.sg

Rene Chew
Liaison Officer
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: Rene_Chew@spf.gov.sg

Ching Yeow Boon
Police Officer
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: CHING_Yeow_Boon@spf.gov.sg

Chng Ho Kiat
Director, Preparedness and Resilience Division
Ministry of Communications and Information
140 Hill Street #01-01A
Old Hill Street Police Station
Singapore 179369
Email: CHNG_Ho_Kiat@mci.gov.sg

Livia Chng
Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: Livia_Chng@nscs.gov.sg

Chok Chin Wee
Engineer
Defence Science & Technology Agency
55 Newton Road, #15-01
Revenue House
Singapore 307987
Email: cchinwe1@dsta.gov.sg

Chua Jia Ying
Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: chua_jia_ying@spf.gov.sg

Jogesh Nambiar Devadas
Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: jogesh_nambiar_devadas@spf.gov.sg

Diong Siew Maan
Principal Psychologist
Singapore Civil Defence Force
91 Ubi Avenue 4
Singapore 408827
Email: Diong_Siew_Maan@scdf.gov.sg

Goh Eng Liang
Immigration & Checkpoints Authority
ICA Building
10 Kallang Road, #08-00
Singapore 208718
Email: goh_eng_liang@ica.gov.sg

Goh Su Kai
Executive (EP)
Ministry of Home Affairs
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: goh_su_kai@mha.gov.sg

Guo Jing Yu, Gabriel
Senior Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: Gabriel_GUO@nscs.gov.sg

Arul Gurusamy
Project Manager
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: Arul_GURUSAMY@mha.gov.sg

Gwee Siow Chui
Lead Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: Evelyn_Gwee@nscs.gov.sg

Saif Haq
Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: saif_haq@nscs.gov.sg

Andrew Ho
Senior Assistant Director, BA (ISTPO)
Ministry of Home Affairs
28 Irrawaddy Rd
Tower M, Level 12
Singapore 329560
Email: andrew_ho@mha.gov.sg

How Khee Yin
Director, Information Division
DSO National Laboratories
20 Science Park Drive
Singapore 118230
Email: hkheeyin@dso.org.sg

Benson Huang
Consultant
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: benson_huang@nscs.gov.sg

Deanna Kim
Political Unit Chief
U.S. Embassy
27 Napier Road|
Singapore 258508
Email: kimdg@state.gov

Kristen Koh
Learning & Development Specialist
Civil Service College
31 North Buona Vista Road
Singapore 275983
Email: kristen_koh@cscollege.gov.sg

Agatha Koh Liang Yi
Senior Public & Internal Communications Executive
Immigration & Checkpoints Authority
ICA Building
4th level Central Registry Mailroom
#04-B-22, 10 Kallang Road
Singapore 208718
Email: agatha_koh@ica.gov.sg

Sunthiya Krishnan
Intelligence Officer
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawady Road
Singapore 329560
Email: Sunthiya_Krishnan@spf.gov.sg

Bhavani Krishnasamy
Managing Director
Vin Public Relations Consultancy
Email: bhavani0902@gmail.com

Kua Choon Jin
Head, Intelligence Analysis & Processing
Singapore Police Force
391 New Bridge Road
Police Cantonment Complex
Singapore 088762
Email: Kua_Choon_Jin@spf.gov.sg

Jerome Kuah
Executive, Media Operations
Ministry of Communications and Information
140 Hill Street Level 4
Old Hill Street Police Station
Singapore 179369
Email: jerome_kuah@mci.gov.sg

Stephanie Kwok
Assistant Director
Ministry of National Development
5 Maxwell Road
#21-00 & #22-00, Tower Block
MND Complex
Singapore 069110
Email: Stephanie_Kwok@mnd.gov.sg

Andrew Lee Chuin Siang
Program Manager
Police Headquarters
Singapore Police Force
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: Andrew_LEE@spf.gov.sg

Edward Lee
NYPD Intelligence Division
New York City Police Department
1 Police Plaza
New York, NY, 10001
USA
Email: elee617@gmail.com

Lee Liang Chye
Police Officer
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: LEE_Liang_Chye@spf.gov.sg

Mexcel Lee
Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: mexcel_LEE@nscs.gov.sg

Sean Lee
Director
Heritage Conservation Centre
32 Jurong Port Road
Singapore 619104
Email: sean_lee@nhb.gov.sg

Lee Tin Hua
Head, SCG4, FSTD
Ministry of Defence
14, Science Park Drive 1
The Maxwell
Science Park 1
Singapore 118226
Email: LEE_Tin_Hua@starnet.gov.sg

Grace Leong
Senior Assistant Director
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: Grace_Leong@nscs.gov.sg

Liaw Koy Fatt
Head, Customer Data Analytics
Ministry of Education
1 North Buona Vista Drive
#10-05
Singapore 138675
Email: liaw_koy_fatt@moe.gov.sg

Avril Lim
Senior Customs Officer
Singapore Customs
55 Newton Road
#10-02, Revenue House
Singapore 307987
Email: avril_lim@customs.gov.sg

Lim Li Yin
Lead Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: liyin.lim@gmail.com

Ling Siew Boon
Staff Officer
Ministry of Defence
303 Gombak Drive
#03-12
Singapore 669645
Email: ling_siew_boon@starnet.gov.sg

Samantha Loh
Assistant Director
Civil Service College
31 North Buona Vista Road
Singapore 275983
Email: samantha_loh@cscollege.gov.sg

Loke Wai Yew
Deputy Commander
Tanglin Police Division
Singapore Police Force
21 Kampong Java Road
Email: loke_wai_yew@spf.gov.sg

Low Woon Pin
Senior Engineer
Defence Science & Technology Agency
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: lwoonpin@dsta.gov.sg

Nur Azlin Mohamed Yasin
Associate Research Fellow
S. Rajaratnam School of International Studies
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: isnurazlin@ntu.edu.sg

Nathan Diane Marie Helen
Information Analyst
Ministry of Defence
303 Gombak Drive
#03-12
Singapore 669645
Email: nathan_diane_marie_helen@starnet.gov.sg

Lal Nelson
Director
Ministry of Home Affairs
New Phoenix Park
28 Irrawaddy Road
M Tower, Level 17
Singapore 329560
Email: Lal_Nelson@mha.gov.sg

Mushahid Ali
Senior Fellow
S. Rajaratnam School of International Studies
Nanyang Technological University
Block S4, Level B4
Nanyang Avenue
Singapore 639798
Email: ismali@ntu.edu.sg

Neo Loo Seng
Senior Behavioural Sciences Research Analyst
Ministry of Home Affairs
501 Old Choa Chu Kang Road
Singapore 698928
Email: neo_loo_seng@mha.gov.sg

Ng Gee Wah
Programme Director
DSO National Laboratories
20 Science Park Drive
Singapore 118230
Email: ngeewah@dso.org.sg

Ng Ming Hwee
Principal Engineer
Ministry of Defence
1 Depot Road, #19-01
Defence Technology Tower A
Singapore 109679
Email: allen.ngmh@gmail.com

Ng Wei Chian
Senior manager
Ministry of Communications and Information
140 Hill Street Level 6
Old Hill Street Police Station
Singapore 179369
Email: ng_wei_chian@mci.gov.sg

Jason Ngian
Engineer
Defence Science & Technology Agency
55 Newton Road
 #15-01, Revenue House
Singapore 307987
Email: jasonngian@hotmail.com

Ong Kuei Fang
Analyst
Singapore Police Force
Police Headquarters
 New Phoenix Park
28 Irrawady Road
Singapore 329560
Email: Ong_Kuei_Fang@spf.gov.sg

Sharma Jon-Paul Parvesh
Analyst
Ministry of Defence
Tanglin Post Office
PO Box 844
Singapore 912499
Email: sharmajonpaul@gmail.com

Peh Cheng Hwee
Assistant Director
Ministry of Education
1 North Buona Vista Drive
Singapore 138675
Email: peh_cheng_hwee@moe.gov.sg

Phang Nyit Sin
Branch Head
Ministry of Defence
303 Gombak Drive, #03-12
Singapore 669645
Email: phang_nyit_sin_michael@starnet.gov.sg

Jane Quek
Psychologist
Ministry of Home Affairs
501 Old Choa Chu Kang Road
Singapore 698928
Email: quek_jane@mha.gov.sg

Praveen Randhawa
Deputy Director, Corporate Communications
Ministry of Law
100 High Street
#08-02, The Treasury
Singapore 179434
Email: Praveen_RANDHAWA@Mlaw.gov.sg

Edawanty Abdul Razak
Head, New Media
Ministry of Education
Corporate Comms Division
20th Floor, 1 North Buona Vista Drive
Singapore 138675
Email: edawanty_abdul_razak@moe.gov.sg

Logapreyan Renganathan
Deputy Director
Communications Group (Liaison)
Prime Minister's Office
5 Maxwell Road
#21-00 & #22-00 Tower Block
MND Complex
Singapore 069110
Email: logapreyan_renganathan@pmo.gov.sg

Kristin Samivelu
Senior Analyst
Ministry of Home Affairs
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: kristin_samivelu@mha.gov.sg

Geraldine Seah
Senior Executive (HCC)/CPD, JOD
Ministry of Home Affairs
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: geraldine_seah@mha.gov.sg

Alan Seow
Head, Risk Assessment
Ministry of Communications and Information
140 Hill Street #01-01A
Old Hill Street Police Station
Singapore 179369
Email: alan_seow@mci.gov.sg

Andrea Shepherdson
Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: andrea_shepherdson@spf.gov.sg

Priscilla Shi
Research analyst
Ministry of Home Affairs
501 Old Choa Chu Kang Road
Singapore 698928
Email: priscilla_SHI@mha.gov.sg

Lincoln Sim
Manager, Marketing Communication
Ministry of Health
16 College Road
Singapore 169854
Email: Lincoln_Sim@moh.gov.sg

Anshul Singhania
Analyst
National Maritime Sense-making Centre
103 Tanah Merah Coast Road
 #01-30
Singapore 498750
Email: anshul_singhania@starnet.gov.sg

Steven Soo
Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawady Road
Singapore 329560
Email: soo_chee_tuck@spf.gov.sg

Tan Chee Seng
Head, SCG1
Ministry of Defence
14, Science Park Drive 1
The Maxwell, Science Park 1
Singapore 118226
Email: TAN_Chee_Seng@starnet.gov.sg

Tan Chee Yong, Adrian
Web Comms Team Leader
Singapore Civil Defence Force
91 Ubi Avenue 4
Singapore 408827
Email: tan_chee_yong@scdf.gov.sg

Eunice Tan
Psychologist
Ministry of Home Affairs
501 Old Choa Chu Kang Road
Singapore 698928
Email: Eunice_Tan@mha.gov.sg

Justin Tan Fun Peng
Assistant Head, Intelligence Branch
Singapore Customs
55 Newton Road
#10-01, Revenue House
Singapore 307987
Email: justin_tan@customs.gov.sg

Gregory Tan
Police Officer
Singapore Police Force
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: Gregory_TAN@spf.gov.sg

Hannah Tan
Assistant Director
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: hannah_tan@nscs.gov.sg

Jackson Tan
Manager, New Media
Ministry of Communications and Information
140 Hill Street, 6th Storey
Old Hill Street Police Station
Singapore 179369
Email: jackson_tan@mci.gov.sg

Jaslynn Tan
Analyst
National Security Coordination Secretariat
55 Newton Road
#15-01, Revenue House
Singapore 307987
Email: jaslynn_tan@nscs.gov.sg

Josiah Tan
Project Manager
Ministry of Defence
AFPN 0067
14 Science Park Drive
The Maxwell, Science Park 1
Singapore 118226
Email: tan_chung_huat_josiah@starnet.gov.sg

Tan Kar Wee
Strategic Communications Executive
Ministry of Education
1 North Buona Vista Drive
Singapore 138675
Email: tan_kar_wee@moe.gov.sg

Tan Wenyi
Police Officer
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: TAN_Wenyi@spf.gov.sg

Tan Yi Wen
Social Media Analyst
National Security Coordination Secretariat
55 Newton Road
Revenue House #15-01
Singapore 307987
Email: wenwhy14@gmail.com

Nicholas Tay
Senior Executive
Ministry of Home Affairs
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: nicholas_TAY@mha.gov.sg

Tee Cheong Siang
Police Officer
Police Headquarters
Singapore Police Force
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: TEE_Cheong_Siang@spf.gov.sg

Alvin Teo
Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: teo_guo_yang@spf.gov.sg

Kym Yeo
Analyst
Ministry of Defence
Tanglin Post Office
PO Box 844
Singapore 912499
Email: yun.kym@gmail.com

Teow Loo Nin
Lab Head
DSO National Laboratories
20 Science Park Drive
Singapore 118230
Email: tloonin@dso.org.sg

Gerald Tham
Concepts & Systems Officer
Ministry of Defence
303 Gombak Drive
#02-34
Singapore 669645
Email: THAM_Zhi_Choong_Gerald@starnet.gov.sg

Thian Yee Sze
Director-General, Legal Group
Ministry of Law
100 High Street
#08-02 The Treasury
Singapore 179434
Email: thian_yee_sze@mlaw.gov.sg

Adrian Toh
Head Field Intelligence Branch, CID
Singapore Police Force
391 New Bridge Road
Police Cantonment Complex Block C
Singapore 088762
Email: Adrain_Toh@spf.gov.sg

Julianne Toh
Analyst
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: julianne_toh@spf.gov.sg

Mano Vikneshwaran
Executive, Public Communications Division
Ministry of Communications and Information
140 Hill Street #01-01A
Old Hill Street Police Station
Singapore 179369
Email: mano_vikneshwaran@mci.gov.sg

Wang Yingmin
Research Analyst
Ministry of Home Affairs
501 Old Choa Chu Kang Road
Singapore 698928
Email: wang_yingmin@mha.gov.sg

Vanessa Wong
Senior Research Officer
Social Change Research
Ministry of Home Affairs
28 Irrawaddy Road
Singapore 329560
Email: vanessa_wong@mha.gov.sg

John Wood
Defense & Naval Attaché
U.S. Embassy
27 Napier Road
Singapore 258508
Email: FinchumLG@state.gov

Karen Yap
Education Officer
Ministry of Education
1 North Buona Vista Drive
Singapore 138675
Email: tay_kai_yun@moe.gov.sg

Ye Hong Xiang
Manager
Ministry of Communications and Information
140 Hill Street #01-01A
Old Hill Street Police Station
Singapore 179369
Email: ye_hong_xiang@mci.gov.sg

Andy Yeo Chin Heng
Head, Operations Programme Management Team
Singapore Police Force
Police Headquarters
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: Andy_C_H_YEO@spf.gov.sg

Vanessa Yeo
Counsel for Parliament Affairs
Ministry of Law
100 High Street
#08-02, The Treasury
Singapore 179434
Email: vanessa_yeo@mlaw.gov.sg

Peter Yew
Head, DSMMG
National Security Coordination Secretariat
55 Newton Road
#15-01 Revenue House
Singapore 307987
Email: peter_yew@nscs.gov.sg

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 globalised, 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/