CROWDSOURCING FOR NATIONAL SECURITY

Policy Report
March 2015

Jennifer Yang Hui

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Policy Report

CROWDSOURCING FOR NATIONAL SECURITY

Jennifer Yang Hui
March 2015

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

Executive Summary

The understanding of national security has expanded beyond the traditional state-centric responsibility to include more players in the society. One of the key arenas of national security operations is now the internet, where user-generated content in the social media combines with offline operations to form crucial intelligence information. Rather than passively looking out for operational information, however, national security practitioners now have the option to invite the public to jointly ensure security by contributing their expertise and knowledge through the internet. The notion of crowdsourcing, first applied to business models, is an open call for contribution from a previously unknown pool of contributors that has proven extremely workable in the information age.

The first part of this paper will discuss several benefits of crowdsourcing. Crowdsourcing is widely believed to be able to provide solutions for any problem an organisation may face in a cost-saving and efficient manner. Furthermore, crowdsourcing through internet helps to find experts and manpower that would otherwise need a degree of effort to find offline. As an added bonus to national security operations, crowdsourcing operations may be done confidentially.

The second part of the paper will follow up by listing some common crowdsourcing platforms and discussing the ways in which they had been employed in recent disasters and national security operations. Many third-party crowdsourcing systems are available on the web, but organisations may opt to customise crowdsourcing systems for their usage. Available case studies show that crowdsourcing has been widely used as a source for intelligence in national security operations. It is also increasingly used to find innovative solutions to challenges to national security such as seeking international experts' assistance in finding solution for securing the cyberspace.

The final section of the paper concludes by discussing possible limitations associated with crowdsourcing in general. Among others, data gleaned from crowdsourcing operations are of varying quality, giving rise to challenges in utilising such non-expert data. It also means challenges in establishing effective incentive mechanism and giving rise to costs, especially in the area of human resource. Decision-makers should also be aware that deploying crowdsourcing essentially means a loss of control over user behaviour and the direction in which the operation may be headed. In interpreting the data, it is also important to note that participation in crowdsourcing operations is generally limited to the middle class who are technologically savvy and educated.

Introduction

Post-September 11th attack on the United States' World Trade Center, national security increasingly recognised the importance of involving many different actors in the society. For instance, Singapore's strategy in the fight against terrorism noted that contemporary national security is complex and involves many entities for effective execution.[1] Similarly, the United Kingdom actively seeks its citizens' cooperation in its counter-terrorism activities.[2] In combating crime and challenges to national security, the importance of public engagement cannot be underestimated.

Given the common interests and mode of operation of engaging the public, this paper suggests that national security has much to benefit from crowdsourcing operations. Crowdsourcing refers to the open sourcing of ideas, innovations and solutions from a large number of people whose identity is usually unknown. The term was first coined by a contributing editor of *Wired* magazine, Jeff Howe, in 2006.[3] Passion for the task at hand appears to be the most important factor in getting the work done effectively and arriving at the most accurate solution. To illustrate, Howe noted that:

> *"Crowdsourcing had its genesis in the open source movement in software. The development of the Linux operating system proved that a community of like-minded peers was capable of creating a better product than a corporate behemoth like Microsoft. Open source reveal a fundamental truth about humans that had gone largely unnoticed until the connectivity of community than it can in the context of a corporation. The best person to do a job is the one who most wants to do that job; and the best people to evaluate their performance are their friends and peers who, by the way, will enthusiastically pitch in to improve the final product, simply for the sheer pleasure of helping one another and creating something beautiful from which they all will benefit."*[4]

While not a novel concept, the advantages of crowdsourcing had been heightened with the advent of the internet and social media.[5] As a collection of internet-based applications that facilitate the creation and exchange of user-generated content, the social media transforms users from consumers to producers of content.[6] The vast amount of data available on social media platforms, with the right mining and analytics technological tools, has already proven useful for solving national security problems. Social media allows crowdsourcing operations to reach a large group of people within a short span of time. They can find experts who may prove valuable to solving certain problems. The social media also makes it easier for users to communicate and collaborate. Additionally, the

---

1 "The Fight against Terror: Singapore's National Security Strategy," *National Security Coordination Centre*, 2004, p. 32.

2 "A Strong Britain in an Age of Uncertainty: The National Security Strategy", *UK Cabinet Office*, October 2010.

3 Jeff Howe, "The Rise of Crowdsourcing", *Wired Magazine*, Issue 14.06, June 2006. Accessed 14 August 2014 http://archive.wired.com/wired/archive/14.06/crowds.html.

4 Jeff Howe, *Crowdsourcing: Why the power of the crowd is driving the future of business* (New York: Crown Business, 2008), p. 8.

5 Ravi Gupta and Hugh Brooks, *Using Social Media for Global Security* (Indianapolis: John Wiley & Sons, Inc, 2013), p. 27. See also Daren C. Brabham, "Crowdsourcing: A Model for Leveraging Online Communities", in Aarn Delwiche and Jennifer Jacobs Henderson (eds.) *The Participatory Cultures Handbook* (New York and London: Routledge, 2013), p. 121.

6 Nicky Antonius and L. Rich, "Discovering collection and analysis techniques for social media to improve public safety", *The International Technology Management Review*, Vol. 3 (2013) No. 1, p. 43.

engaging nature of multimedia that many of the social media platforms utilise is attractive to users.[7] Therefore, social media makes a natural complement to crowdsourcing platforms, with the latter often being incorporated within existing social media platforms. Custom-built crowdsourcing platforms also involve the social media.

7 Gupta and Brooks, *Using Social Media for Global Security*, p. 184.

Why Crowdsource?

1. Tapping on the crowd's potential: manpower, expertise and innovation

The benefits of crowdsourcing lay mainly in the "wisdom of crowds". The theory suggests that the average response of many people, even amateurs, to a question is frequently more accurate than the views of a few experts.[8] In this respect, a community of individuals with common interests and facing the same tasks are capable of delivering better products and solutions than experts alone in the field. Information systems scholars Jean-Fabrice Lebraty and Katia Lobre-Lebraty confirmed that the "diversity and independence of the members of a crowd" is a value addition to crowdsourcing operations.[9]

Therefore, the advantages of crowdsourcing lie mainly in the innovative ideas and problem-solving capacity that the diverse contributors — which may consist of experts and interested amateurs — can provide. The crowd can provide expert and faster solution to an existing problem. Depending on the challenge at hand, the solution provided may also prove innovative.

2. Cost savings

Crowdsourcing operations are cost-efficient compared to outsourcing of work.[10] Due to the easy availability of technology, it is inexpensive to establish a web page, smartphone application or send a mass text to a group of people. Additionally, the platform can be easily closed down or adapted to new functions after the completion of the crowdsourcing project.[11] Therefore, the technology and administration of crowdsourcing operations generates savings for the organisations in terms of costs.

3. Work discreetly

National security values confidentiality in its operations. Crowdsourcing platforms make excellent medium for discreet intelligence collection.[12] The protection of the identity of informants will greatly aid the collection of information that will be useful for national security operations. Building customised crowdsourcing platforms is especially useful to avoid possible obstacles of lack of cooperation from established social media platforms. Social media platforms may refuse to reveal too much of their users' data required for investigation.[13] They may also limit the type as well as the amount of data that national security officers may obtain.[14] In addition, creating customised crowdsourcing platforms also help in limiting the access to data that may be potentially sensitive or private.[15]

---

8 See James Surowiecki, *The Wisdom of Crowds: Why the Many are smarter than the Few and How Collective Wisdom shapes Business, Economies, Societies and Nations* (New York and Auckland: Doubleday, 2004).

9 Jean-Fabrice Lebraty and Katia Lobre-Lebraty, *Crowdsourcing: One Step Beyond* (London and New Jersey: ISTE Ltd and John Wiley & Sons, Inc, 2013), p. 23.

10 See Lebraty and Lobre-Lebraty, *Crowdsourcing: One Step Beyond*, p. 34 and Doug Tewksbury, "Crowdsourcing Homeland Security: The Texas Virtual BorderWatch and Participatory Citizenship", *Surveillance & Society* Vol 10(2012) No. 3/4: 249-262.

11 Gupta and Brooks, *Using Social Media for Global Security*, p. 186.

12 Ibid.

13 Ibid, p. 194.

14 Ibid, p. 192.

15 Ibid.

Crowdsourcing for National Security and Law Enforcement

Crowdsourcing is useful for national security and law enforcement operations for two main purposes: (i) sourcing for intelligence and (ii) finding innovative solutions to security challenges.

Sourcing for Intelligence

Crowdsourcing may be used to tap on users' knowledge for timely and relevant data in crisis situations. For instance, in the aftermath of the riots in the U.K. in 2011, photos of those suspected of looting were uploaded onto Flickr, a photo-sharing platform, as well as a dedicated website was set up specifically for the purpose of suspect identification. Additionally, nearly 2,800 photos were uploaded onto the smartphone app Facewatch ID. It allowed users to sort the photos according to postal codes and inform the authorities whenever they recognise someone among the posted pictures.[16] London Metropolitan Police (MET) and Greater Manchester Police (GMP) employed Twitter for supporting investigations and to find information on offenders. On 12 August 2011, GMP launched an online crowdsourcing campaign for information on looters using Twitter. The hashtag #shopalooter was used. The public could submit their input via the phone numbers and links provided on the website, as well as Twitter messages.[17] This led to the arrest of 770 people and the charging of 167.[18]

In the United States, one example of crowdsourcing for law enforcement was the establishment of the Texas Virtual Border Watch for the defence of the U.S.-Mexico border.[19] This comprised of placing a series of governmental web-based surveillance cameras at the border. Any users with internet connection may watch the surveillance videos and report any criminal activities such as drug smuggling and illegal immigration through the system.

The U.S. Department of Homeland Security also established the Neighbourhood Network Watch programme that aimed to collect data on online criminal behaviour by encouraging its citizens and organisations to report suspicious online activities.[20]

Recent crowdsourcing projects also allowed scenario planning for risk assessment. Wikistrat, which calls itself the world's first crowdsourced analytical services consultancy, employs the services of a closed group of subject experts and has been helpful in solving some issues pertaining to national security.[21] For example, the company was hired to study and see if the Islamic State (IS) would infiltrate Jordan and the means in which they may do so. Forty-five international experts on the Middle East from academic, diplomatic and military backgrounds brainstormed potential scenarios real-time on Wikistrat's online platform and came out with a few scenarios on the IS's next move as well as its likelihood of occurring. Their assessment included the following scenarios: (i) the attempted capture of Amman by the IS; (ii) IS effort to cause discontent among citizens with regards to the peace treaty between Jordan and Israel; and (iii) recruitment of such discontented individuals.[22]

---

16 Facewatch ID website, accessed on 01 December 2014 http://facewatchid.co.uk/

17 Sebastian Denef, Petra S. Bayerl and Nico Kaptein,"Social Media and the Police_ Tweeting Practices of the British Police Forces during the August 2011 Riots", *Conference on Human Factors in Computing System*, 2013, accessed 25 April 2014 http://www.fit.fraunhofer.de/content/dam/fit/de/documents/ukriots%20v90.pdf.

18 Jamie Bartlett and Carl Miller, "The State of the Art: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism", *DEMOS*, November 2013, p. 48. See also Denef, Bayerl and Kaptein,"Social Media and the Police", 2013.

19 Tewksbury, "Crowdsourcing Homeland Security", pp. 249-262.

20 Gary M. Shiffman and Ravi Gupta, "Crowdsourcing cyber security: a property rights view of exclusion and theft on the information commons," *International Journal of the Commons*, Vol. 7 (February 2013) No. 1, p. 106.

21 Wikistrat website, accessed on 03 November 2014 http://www.wikistrat.com/.

22 Aaron Stanley, "With Wikistrat, crowdsourcing gets geopolitical," *Financial Times*, 03 September 2014.

The U.S. Africa Command also used Wikistrat to run a simulation exercise on illicit trafficking activities in the Trans-Sahel region.[23] The positive feedback of the organisation noted that crowdsourcing was able to process large amounts of information at a faster pace.

Finding Innovative Solutions to Security Challenges

National security organisations have used crowdsourcing to seek innovative solutions to challenges faced in their line of work. For example, the U.S. Defense Advanced Research Projects Agency (DARPA) has been the forerunner of several crowdsourcing challenges in the security arena. The most famous example was the Red Balloon Challenge or Network Challenge. The organisation offered a reward of US$40,000 to those who could submit the correct information of the location of each balloon. The winner was a team from the Massachusetts Institute of Technology (MIT), who crowdsourced the balloons' locations through the social media. The Red Balloon Challenge showed the strength of crowdsourcing that leveraged on social networks, allowing the collection of intelligence and solution to challenging issues.[24]

DARPA's other project, the Shredder Challenge was launched in late 2011 to find suitable computer algorithms to reassemble and interpret shredded documents.[25] A website was launched in which pictures of shredded documents were posted and users worldwide invited to reassemble the documents. In addition, DARPA utilised social media platforms to inform netizens about the challenge, promising a reward of US$50,000 to the winner. The challenge managed to attract the participation of 9,000 teams. The winner of the challenge was a team of computer programmers from San Francisco, who solved the challenge in 33 days.[26]

More recently, in 2013 the U.S. State Department organised a contest — the Innovation in Arms Control Challenge — which sought ideas on how crowdsourcing can support arms control transparency.[27] The winner of the challenge, who received US$10,000 for his participation, proposed the usage of visible light communications (VLC) to improve and expedite arms control inspections.

The British government is also one of the pioneers in crowdsourcing for national security. One interesting project was undertaken in 2011 by the Government Communications Headquarters (GCHQ), the British intelligence organisation, which launched a crowdsourcing challenge on *www.canyoucrackit.co.uk* with the aim of recruiting signal intelligence officers who possess the aptitude for cracking codes. The website was interactive, allowing for two-way communication. The operation used Facebook to advertise the effort.[28] Participants were required to solve a code of 160 letters and numbers arranged in a rectangular display. Once solved, the participants would receive a keyword that led to another website, which would allow them to apply for a position in the GCHQ.

Crowdsourcing has also been applied for securing the cyberspace. The U.S. Department of Homeland Security (DHS) and the Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California had funded a study that showed the advantages of crowdsourcing for cybersecurity.[29]

---

23 Ibid.

24 Gupta and Brooks, *Using Social Media for Global Security*, p. 190.

25 Ibid, p. 189.

26 Ibid.

27 "Innovation in Arms Control Challenge", *U.S. Department of State*, accessed 22 September 2014 http://www.state.gov/t/avc/innovationcompetition/.

28 Gupta and Brooks, *Using Social Media for Global Security*, p. 190.

29 See Shiffman and Gupta, "Crowdsourcing cyber security," pp. 92-112.

The research argued that the current attribution and audit frameworks for the prevention of cyber criminality and attackers is limited and unable to keep up with the innovative ways in which cyber criminals and spies mask their identity online. The centralised system of the current attribution model also increases vulnerability. Furthermore, the attribution model is costly and cannot keep up with the rapid speed in which computer viruses spread on social networks and hardware.[30] Instead, a method that involves "treating the internet as a commons and encouraging individuals and institutions to voluntarily implement innovative and adaptive monitoring mechanisms" appeared to be more effective in securing the cyberspace.[31] For example, a group of volunteer experts from America Online, Symantec, Georgia Institute of Technology, Shadowserver Foundation, Internet Corporation for Assigned Names and Numbers, and China's Ministry of Information Industry worked together to find a solution to the challenge of the Conficker computer virus, which was discovered in November 2008. Using only a website, e-mail mailing lists and conference calls, the group developed a software that was able to detect the presence of the virus on infected computers and eliminate it. In addition, they also came close to identifying the creator of the virus, who was believed to be from Ukraine. [32]

---

30 Ibid, p. 96.

31 See Shiffman and Gupta, "Crowdsourcing cyber security", pp. 92-112.

32 Ibid, p. 105.

Crowdsourcing Platforms

Crowdsourcing platforms are relatively new to social media; however, the principles behind the concept have been in place since the birth of social media. Social media platforms crowdsource information about its users and their networks, with the intention of forwarding the information to other social media platform users and advertisers. Crowdsourcing is also becoming a specific solution and information set for some websites such as Wikipedia and the U.S. government's challenge.org website, which crowdsources solutions to U.S. government's problems.[33] Crowdsourcing platforms include mediums such as standalone websites, smartphone applications and SMS-based communication networks.[34]

In developing crowdsourcing systems, organisations may choose between developing their own crowdsourcing platforms or relying on third-party systems. Most of the Web 2.0 technologies such as wikis, tagging functions, mashups, blogs, RSS filters, podcasts and SNS may be used to design the interfaces and backup platforms for crowdsourcing systems. Some examples of third-party crowdsourcing platforms include:

(i) Amara (http://amara.org/en/): a platform for translations.

(ii) Amazon Mechanical Turk (https://www.mturk.com/mturk/welcome): an online platform that allows users to either crowdsource other users to complete a particular work or to find work to be done. Tasks to be done are called Human Intelligence Tasks (HITs) and include work such as translation, rating or tagging pictures, videos and music.[35]

(iii) InnoCentive (http://www.innocentive.com/): a website that allows client companies to crowdsource solutions to the challenges they are facing.

(iv) Crowdflower (http://www.crowdflower.com/): a similar platform to Amazon Mechanical Turk, which allows the crowdsourcing of tasks.

(v) GeoChat (http://instedd.org/technologies/geochat/): an online tool that allows users to chat, report and receive alerts on their smartphones.

(vi) Ushahidi (http://www.ushahidi.com/): an open source platforms that enable interactive mapping applications with Web forms/e-mail, SMS and Twitter support. It is also available on mobile apps for smartphones and tablets.[36]

(vii) Indiegogo (https://www.indiegogo.com/): a crowdfunding website. It was recently used to raise US$5 million for independent investigation into the cause of MH370 crash.[37]

(viii) Tomnod (http://www/tomnod.com): It is a crowdsourcing website run by DigitalGlobe. Inc that crowdsourced for help from more than 2 million people to look through satellite images for the missing Malaysian Airlines MH370.[38] By 13 March 2014, approximately 645,000 features had been flagged.[39]

---

33 Gupta and Brooks, *Using Social Media for Global Security*, pp. 27-28.

34 Ibid, p. 182.

35 Stevan Rudinac, Martha Larson, and Alan Hanjalic, "Learning Crowdsourced User Preferences for Visual Summarisation of Image Collections, *IEEE Transactions on Multimedia*, Vol. 15 (October 2013) No. 6, p. 1234.

36 Kamel Boulos, et. al. "Crowdsourcing, citizen sensing and sensor web technologies for public and environmental health surveillance and crisis management: trends, OGC standards and application examples", *International Journal of Health Geographics* 10 (2011):67.

37 Indiegogo website, accessed 19 January 2015 https://www.indiegogo.com/.

38 Robert Fenner, "Satellite Crowdsourcing Adds 2 Million Searchers for Missing Jet," *Bloomberg.com*, 13 March 2014, accessed 28 July 2014 http://www.bloomberg.com/news/2014-03-13/satellite-crowdsourcing-adds-2-million-searchers-for-missing-jet.html.

39 Ibid.

Problems in utilising non-expert data

Government agencies, including national security organisations, need to increasingly incorporate citizen-contributed data in their work. Geographer Michael Goodchild observed that contemporary government organisations use two types of data. The first is provided by non-paid volunteers who are also non-experts and the data generated is therefore, at times, questionable in terms of their sources. Crowdsourced data falls under this category. The second type of data is collected by hired experts on the subject as part of a formal framework of research and the resulting data may still suffer from error, but its source is known.[40] However, utilising information from public-volunteered data is different from traditional data that is collected and analysed by experts; crowdsourced data needs a paradigm shift on the part of government bodies. In their discussion of volunteered geographic information (VGI), geographers Peter Johnson and Renee Sieber noted that: "Governments face a formidable challenge in accepting VGI when they shift from the use of only expert data to a mixed model that can evaluate and incorporate citizen volunteered data. This shift requires that governments engage with several aspects of the VGI creation process, including the individual contributors of VGI, a step towards widespread participation that many in government may not be ready to take."[41]

Irrelevant input

The social media is a "noisy" medium, comprising of both valid and irrelevant information. While crowdsourcing operation for national security seeks credible and, at times, expert input, the design and scope of the platform may attract unhelpful contribution. For example, depending on the objectives of the operation, amateur contributions may yield useful insights, however, the data may prove unhelpful.

"Foolishness of the Crowd"

While the benefit of "wisdom of the crowd" has been much touted, the crowd does not always provide the most accurate or helpful solution in crowdsourcing projects. As health informatics scholar Kamel Boulos argued:

> *"Crowdsourced data have a tendency to be resistant to nuance and correction; especially in social media, once a meme snowballs in the 'echo chamber', it can be very hard to correct (or 'counter-tweet') and the crowd is sometimes not so fast at changing course;…Crowds often have no immediate way to discern truth from falsehood; what gets propagated is the 'popular' opinion shaped by the most prominent personalities, beliefs and agendas of the individuals in the 'crowd'… Crowds are prone to add opinion to data; which sometimes sticks more than the credible data themselves. Separating opinion and credible data through expert interpretation and curation, both centralized and decentralized, is important (in decentralized curation, specific statements of fact are expressed or extracted from citizen-generated information are validated, refuted, and expanded by the citizens themselves in a more distributed system."*[42]

---

40 Michael F. Goodchild, "Citizens as Sensors: The World of Volunteered Geography", 69 *GeoJournal* (2007):211-221.

41 Peter A. Johnson and Renee E. Sieber, "Situating the Adoption of VGI by Government", in D. Sui et al. (eds.), *Crowdsourcing Geographic Knowledge: Volunteered Geographic Information (VGI) in Theory and Practice* (New York and London: Springer Science+Business Media Dordrecht, 2013), p. 72.

42 Boulos, et. al. "Crowdsourcing, citizen sensing and sensor web technologies", p. 67.

"Foolishness of the crowd" will therefore result in irrelevant and unhelpful information as opposed to benefits of the wisdom of the crowd.[43] In addition, social media users tend to add opinion in their contributions to the various platforms. Opinion may be objective and worthy of being used for analysis. However, they may also be unreliable. For instance, the role of peer pressure on opinion needs to be taken into account in analysing crowdsourced data.[44] Information cascading, a situation whereby opinion about a particular service or product was influenced by others, may result in a less than objective evaluation.[45]

Less skilled input

Contributors to crowdsourcing operations involve expertise from many different levels and may include non-experts and amateurs. There is the question of how to tap better into the potential benefits of experts while ignoring the less skilled inputs.

Sampling Bias of Social Media Users

Social media usage is at present still largely restricted to the middle and upper class living in urban areas that possess computers and smartphones.[46] This phenomenon leads to selection bias in utilising social media data as some segment of the population may be left out and therefore is not suitable for crowdsourcing, which relies on the internet and social media.

Challenges of two-way communication: operational security versus central control

The cultural values underpinning social media and national security are widely different. While the former is based on openness and informality, the latter needs command and control, hierarchy and operational security to operate.[47] There is therefore deep-seated suspicion of social media among some segments of the national security community. In view of such perceptions, Bartlett and Miller advised that "any form of appropriate engagement with the public on social media requires a number of risks to be addressed and managed."[48]

In this respect, Ravi and Gupta noted that crowdsourcing is not advisable in two situations. The first is the case when confidentiality and secrecy is paramount to the operation at hand, a situation that may be compromised by the ease of access by social media users.[49] Secondly, if the organisation's tolerance for risk is very low and is afraid of the effect of open interaction online, it may not be advisable to run crowdsourcing platforms that allow user interaction.[50] Crowdsourcing is ultimately about engagement and thus require stakeholders to cede control to users.

Costs

While crowdsourcing is generally touted to be cost-saving in comparison to other forms of operations, it does incur its own costs in terms of financial, software and services. In addition, crowdsourcing operations may incur human resource costs for training to negotiate the learning curve for adopting the crowdsourcing platform and as well as hiring additional staff for supporting the gathering process.[51]

---

43 Lebraty and Lobre-Lebraty, *Crowdsourcing: One Step Beyond*, p. 98.

44 Ibid, p. 99.

45 Radhika Jain, "Investigation of Governance Mechanisms for Crowdsourcing Initiatives", *AMCIS 2010 Proceedings*, Paper 557, accessed 04 November 2014 http://aisel.aisnet.org/amcis2010/557.

46 Nadia Naviwala, "PakVotes: A Social Media Experiment in Elections Monitoring", *United States Institute of Peace (USIP) Peace Brief No. 171*, 11 April 2014.

47 Bartlett and Miller, "The State of the Art", p. 47.

48 Ibid.

49 Gupta and Brooks, *Using Social Media for Global Security*, p. 193.

50 Ibid.

51 Johnson and Sieber, "Situating the Adoption of VGI by Government", p. 70.

Establishing effective incentive mechanisms

Crowdsourcing operations need to establish effective incentive mechanism so as to attract the desired contribution. To establish the most suitable incentive mechanism for a particular crowdsourcing project, the nature of the target crowd must be understood. Lebraty and Lobre-Lebraty observed that the "crowd" from which crowdsourcing operations draw their value from can be broadly categorised into three communities:[52]

(i) *passionate-skilled*: driven by intrinsic motivations such as altruism or faith in the cause, thus needing less outward motivators such as financial compensation. This group possesses variable but limited level of skills range;

(ii) *skilled-passionate*: seeking material satisfaction such as financial remuneration, this group has variable but tendency towards high level of skills; and

(iii) *hybrid*: those who participate in crowdsourcing operations for largely undefined reasons; they are neither driven by passion for the cause nor financial remuneration. This group tends to be motivated by individual status and visibility.

Gupta and Brooks concurred that the type of incentive should be tailored to the type of target crowd in the crowdsourcing operation. They identified two forms of incentive mechanisms: extrinsic and intrinsic incentives.

(i) *Extrinsic incentives* compose of material items or objects such as money or SMS credits. The authors observed that: "… extrinsic incentives are easy to quantify, measure, inform the target audience about, and provide. …They are also likely to entice participants in the beginning when the platform is first launched and they do not yet trust you. However, extrinsic incentives can become expensive and lose their appeal over time. …In general, when creating a platform for a long period of time, phase out or minimise the role of extrinsic incentives and replace them with intrinsic incentives."[53]

(ii) *Intrinsic incentives* are internally generated motivations that differ from individual to individual, such as pride and sense of ownership from contribution. Gupta and Brooks noted that: "Intrinsic incentives have enormous potential and power. Most people will respond strongly to them and, if given the opportunity, surpass participation expectations. Because much of intrinsic incentives have to do with social factors, such as maintaining reputation and relationships, their propagation among participants will lead to the development of strong communities on the platform, which in turn will lead to the development of strong communities on the platform, which in turn lead to sustained participation."[54] They believe that intrinsic incentive is more effective for maintaining participation for a longer period of time. However, it is more difficult to cultivate and deliver than extrinsic incentives.

---

52 Lebraty and Lobre-Lebraty, *Crowdsourcing: One Step Beyond*, pp. 35-39.

53 Gupta and Brooks, *Using Social Media for Global Security*, p. 210.

54 Ibid, p. 211.

Conclusion

This paper evaluates the advantages of crowdsourcing for national security and weighs these against some challenges faced in employing the method. The benefits of crowdsourcing are well-documented in the media and scholarship; crowdsourcing allows national security organisations to find experts and innovative solutions to challenges in a quick and efficient manner. Creating and deploying crowdsourcing systems are also relatively cost-efficient. An added bonus to the national security community is the fact that crowdsourcing allows discreet collection of data.

Despite the much-touted benefits, the challenges facing crowdsourcing have been given less attention. For one, incorporating non-expert data, which may contain irrelevant and less skilled input or be otherwise biased in one way or another, for governmental organisations remain challenging. Solutions derived from crowdsourced systems may also be unable to capture diverse viewpoints due to the fact that the crowd involved tends to be the middle-class with access to education and technology. Crowdsourcing would require that organisations develop effective incentive mechanism that is able to attract the right kind of crowd for the issue at hand. While generally regarded as cost-saving, it also incurs other forms of costs, especially in the human resources area. Particularly pertinent for national security organisations that values hierarchy and operational security is the fact that crowdsourcing often means giving up some levels of control over the reaction of the crowd and possibly, outcome of the project. Drafting the aims and objectives of any crowdsourcing operation should therefore carefully consider its pros and cons.

The paper also discussed some existing third-party crowdsourcing platforms as well as the ways in which crowdsourcing has been deployed in recent national security operations. Generally, crowdsourcing has been used to collect data for intelligence and to seek innovative solutions to national security issues.

About the Author

Jennifer Yang Hui is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS *raison d'être* is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information about CENS, please visit **www.rsis.edu.sg/research/cens**.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit **www.rsis.edu.sg**.

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg