RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 166 – 12 September 2017

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical issues and contemporary developments. The views of the authors are their own and do not represent the official position of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced electronically or in print with prior permission from RSIS and due recognition to the author(s) and RSIS. Please email: RSISPublications@ntu.edu.sg for feedback to the Editor RSIS Commentary, Yang Razali Kassim.

The Humanitarian Access Paradox: Data Security in Contested Settings

By Martin Searle

Synopsis

In complex humanitarian settings, potential data thieves include warring parties. Beyond undermining privacy, data loss risks violating neutrality, an often critical principle for negotiating humanitarian access. Can aid organisations protect that information?

Commentary

THIS YEAR'S high profile cyberattacks - WannaCry, Petya, notPetya – continue a clear trend. In 2016, the US Democratic National Committee infamously had tens of thousands of emails stolen. The same year, the US Office of Personnel Management was breached for a second time, with attackers targeting personal information of military and intelligence personnel applying for security clearance. In 2015 the Philippines' Commission on Elections' entire database was hacked.

Attacks threaten all organisations adopting new data integration technologies. Humanitarian organisations face particular challenges. As the region considered most at risk from natural disasters globally, there is strong motivation in the Asia-Pacific to integrate humanitarian data systems to drastically reduce human fatalities. Over the past decade, disaster-induced deaths tripled in the region, according to the United Nations. These systems promise better information management leading to greater reduction of suffering and saving of life.

Negotiating Access: The Asian Disaster Setting

Simply collecting data already raises questions of privacy that are familiar to all those considering the integration of their data management systems. Humanitarian organisations must contend with the added concern of collecting data on the most vulnerable, which complicates consent and exacerbates the real world implications of any data breach.

One particular reality of humanitarian work creates peculiar implications in a world where even the most sophisticated of governments are being hacked: the need to negotiate access to – and maintain acceptance in – areas where people in need can reach you.

This region's experiences with natural disasters in areas with ongoing insurgencies underscore the significance of this. Despite the impressive cessation of respective hostilities in northern Sri Lanka and Aceh following the 2004 Tsunami, the conflict still complicated people's ability to reach aid immediately following the disaster. In Sri Lanka, this further deteriorated when the conflict reignited during the longer recovery phase.

In 2012, Typhoon Bopha swept through several areas of Mindanao, Philippines affected by low-intensity conflict between the government and the Moro Islamic Liberation Front. This included Marawi City, parts of which remain under the control of insurgents at the time of writing. This adds new complexity that humanitarians already face in negotiating access to populations in need, and would have clear relevance were a natural disaster to strike the area now.

Core Humanitarian Principles: More Art Than Science

On an almost annual basis, opposition-held areas in Shan and Kachin state, Myanmar, suffer often severe flooding, with the distribution of assistance again complicated by conflict. Indeed, in 2015 a member of the Myanmar Red Cross was tragically killed following an attack on his convoy in Shan State.

Negotiating access in such contexts is more art than science. It involves convincing those with the power to block it that a humanitarian presence adds value in some way they consider significant, and will not provoke excessive negative side-effects. Improved operational effectiveness born of better data technologies would, in most instances, help strengthen the case for allowing aid in. But crucially, it might increase undesirable ancillary impacts.

There are three core humanitarian principles: impartiality, independence and neutrality. Together, independence and neutrality ground the case that the presence of a humanitarian organisation will not entail negative consequences to those with the power to block access.

Maintaining independence allows organisations to argue that their actions do not conform to anyone else's agenda; neutrality ensures that humanitarian assistance and civilian protection will not advantage one side of a political disagreement or conflict.

Paradox of Access

As humanitarian organisations adopt new systems technologies to improve their collection, processing and analysis of information, the value of their assessments becomes increasingly strategic. Analyses of socio-political trends, actor networks and resource capabilities as well as data on movements or key health indicators could all represent actionable intelligence to other political actors.

As such, humanitarians become more tempting targets for cyber-attack. Several NGOs working in or on Syria are already believed to have been targeted by hackers seeking to harvest information they possess.

Thus new integrated systems technologies create a paradox for negotiating access. They strengthen a humanitarian organisation’s bargaining power. But simultaneously, they undermine neutrality by facilitating production of strategic intelligence that is vulnerable to theft.

Would those actors – state and non-state – cited above in Aceh, Sri Lanka, Mindanao and Shan and Kachin states, still consent to humanitarian access during a natural disaster or any other humanitarian emergency if they perceive a risk of aid agencies unwittingly leaking valuable information to their opponents?

Data: To Collect or Not to Collect?

Humanitarian organisations have hitherto not prioritised cybersecurity. Doing so requires expertise they generally do not possess, and redirecting resources away from aiding people directly. Budgets are already stretched across simultaneous famine threats in South Sudan, Somalia, Nigeria and Yemen, and the largest global refugee burden since the Second World War. But cybersecurity cannot be ignored; it has implications on the vulnerability of those in need, and on organisations’ own ability to negotiate access.

In a world where even the most sophisticated of governments are unable to protect their data, the humanitarian community faces a real challenge. Humanitarian organisations must carefully consider what data they collect. In each case they must decide whether the value of collecting and processing any given data for improving their aid effectiveness is outweighed by the risk posed by its loss.

This loss could be both to individuals being assisted and to the organisation’s ability to maintain its negotiated access. This could result in discarding data that would otherwise be useful. Clearly, this will often be an extremely difficult calculation to make. However, much of the promise held by new humanitarian data technologies depends on it.

Martin Searle is Associate Research Fellow with the Centre for Non-Traditional Security (NTS) Studies at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.