The Dichotomy of Technology in Conflict

Beauty and the Beast

Anahi Ayala

Introduction

In the field of Information and Communication Technology for Development there is often a debate rooted in the dichotomy between the highly enthusiastic view of technology, as an enabler of information exchange that bypasses traditional gatekeepers such as broadcasting media and governmental agencies; and the highly pessimistic view, that focuses on the dangers of technology such as technical gaps, the digital divide and privacy and security threats.

The truth is somewhere in between. Particularly in conflict situations, the reality is much more complicated. On the one hand, technology, and mobile technology in particular, allows for immediate and broad early warning systems to be created in places where real-time communication would previously have been almost impossible (see Porcaro and Walker, pp. 33-36; see also Mayo, pp. 46-50). On the other hand, the way information moves in those contexts can affect the deepening of already existing divisions and the further polarisation of opposing views, where technology enables both an immediacy and increase in volume of material feeding specific viewpoints. One of the most important ways in which these phenomena play out in humanitarian environments today is in the ways in which affected communities use and experience technology, particularly in conflict environments (see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31). This article explores the polarising effect of communications systems that are becoming increasingly 'closed'.

From a security management perspective, this same dichotomy is even more accentuated. On one side technology is allowing a broader and larger reach for monitoring security and conversations happening on the ground that can give us real-time insights on risks (see Sambuli and Awori, pp. 27-31); on the other side technology is posing new risks for humanitarian organisations and creating new systems that bypass the usual communication streams and are therefore hidden. The ability to predict violence and provide real-time support in case of violent incidents is strictly related to both our ability to use technology to monitor the situation on the ground, and also to understand how others may be using it to organise violent actions or to create tension.

The link between violence, conflict and technology, especially its use by affected communities and parties to conflict, is only beginning to be understood and the available evidence is in some ways contradictory. In a study that looked at the correlation between the availability of mobile technology and violence, Shapiro and Weidmann (2012)[43] found that in the case of Iraq, the location of cell phone towers is inversely associated with violence: i.e. that areas of greater access to telecommunications experienced less violence. Using district level data and a difference-in-difference design (a research method for estimating causal effects), the authors find that the expansion of the cell phone network in Iraq is associated with decreases in successful violent attacks by insurgent forces. Shapiro and Weidmann (2013) state that this is due to the extensive use of cell phone surveillance by U.S. and Iraqi anti-insurgent forces as well as successful whistle-blower programs. Similarly, in the African context, Livingston (2011)[44] argues that while cell phones might empower violent groups and produce more violence, there is a potential for a reduction in violence if improved monitoring is done by international peacekeeping or governmental forces. Such efforts have been rare so far, however.

[43] Shapiro, J. N. and Weidmann, N. B. (2013). *Is the phone mightier than the sword? Cell phones and insurgent violence in Iraq*. Department of Politics and Woodrow Wilson School, Princeton University. Available from: https://webspace.princeton.edu/users/esocweb/ESOC%20website%20publications/SW_CellphonesIraq.pdf. [Accessed 1 Sept. 2014].

[44] Livingston, S. (2011). Africa's Evolving Infosystems: A Pathway to Security and Stability. *Africa Center for Strategic Studies*. Research Paper No. 2.

Alternatively, Pierskalla and Hollenbac (2013)[45] provide evidence to show that cell phone technology can increase the ability of violent groups to overcome collective action problems in Africa. In particular, they state that cell phones lead to a boost in the capacity of groups to communicate and monitor in-group behaviour, thus increasing cooperation. They offer some insights suggesting that the exploration of potential interactions with country or group-level variables can further illuminate the effects of communication technology on violence.

Pierskalla and Hollenbac conclude that enlarging the communication network of violent groups as well as increasing the rate of communication by group members should raise in-group trust between individual participants. The possibility for fast and easy communication boosts the propensity for and rate of information sharing within groups, creating a shared awareness among group members. This system can also be applied to ethnic groups, religious groups or specific sectors of the population. As Shirky (2008, 51) writes, collective action is critically dependent on group cohesion.[46] The expansion of within-group communication is likely to foster shared beliefs and awareness of groups, thus providing one channel of easing collective action. The higher rate of communication between individual group members also makes the transmission of messages and instructions from group leaders through the decentralised network more likely and efficient. Furthermore, the increase in two-way communication vastly raises opportunities for monitoring each other's behaviour (see Sambuli and Awori, p. 29).

Homophily or the closed network effect: a study from the Central African Republic

An example of this phenomenon is currently playing out in the Central African Republic. The Central African Republic has a mobile coverage of 30% and an Internet penetration of 0.1%. Internews is an international non-profit media organisation whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect, and the means to make their voices heard. In the Central African Republic, where Internews has been working since 2010, the organisation works mainly with radio stations – as radio is without any doubt the most widespread medium of communication in the country, and in certain cases, the most trusted.

Even now, when more than 50% of the radio stations have been looted or destroyed, radio remains the only means to broadly reach the local population. But while technology use in the Central African Republic is not yet widespread, certain technology is available and at low cost. A fake Blackberry on the black market costs 15,000 CF (almost 32 USD). Other phones, either with or without Internet capability, cost around 12,000 CF (or 24 USD). Those phones have two things in common: a camera to take pictures and video, and Bluetooth.

In 2014 a new phenomenon emerged in the country: young people were taking video of massacres and killings with their phones to share with friends and peers. Especially in the capital of Bangui, youth began gathering in groups to share videos and pictures of the violence happening in their areas by using Bluetooth, or sometimes by exchanging memory cards. This information flow is a completely closed and untapped one, where access is gained through a shared view of the conflict or geographical and ethnic commonalities. In other words, access to the circle of information comes from having already been a part of it.

This system is typical of the phenomenon of 'homophily', as discussed by Ethan Zuckerman in his closing remarks at the 2014 PeaceTech conference in Boston [47] and increasingly a hallmark of modern conflicts. The homophily principle states[48] that people's personal networks are homogeneous with regard to many socio-demographic, behavioural, and intrapersonal characteristics. Therefore homophily limits people's social worlds in a way that has powerful implications for the information they receive, the attitudes they form, and the interactions they experience. Within this same context, ties between non-similar individuals also dissolve at a higher rate, which sets the stage for the formation of niches (localised positions) within social space. Use of social media and other closed systems for sharing information mean that digital social networks frequently become ways to reinforce views, limit exposure to alternative narratives and thus reduce dialogue and mutual understanding between groups in conflict.

The consequence is that conversations enabled through homophilic systems are more and more polarised towards one unique vision, the vision of the people forming the network. Within the network, the likelihood of a divergent opinion or conversation that

[45] Pierskalla, J. H. and Hollenbach, F. M. (2013). Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa. *American Political Science Review*. 107. pp. 207-224. Available from: http://polisci.duke.edu/uploads/media_items/technology-collectiveactioncellphoneviolence.original.pdf. [Accessed 1 Sept. 2014].
[46] Shirky, C. (2008) *Here Comes Everybody: The Power of Organizing Without Organizations*. Penguin Press.
[47] Video at https://www.youtube.com/watch?v=Mj_SKNQX654. [Accessed 1 Sept. 2014].
[48] McPherson, M., Smith-Lovin, L. and Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology*. 27 (1). pp. 415-444.

presents opposing or different opinions is minimised. The information received in those networks is likely to be aimed at enforcing and supporting a singular point of view, and less likely to be surprising or challenging. Common ground between sides in a conflict is therefore reduced.

This is exactly the situation we observe now in the Central African Republic, where Bluetooth is being used to create a closed information system that can function without Internet and still diffuse information that appeals to people sharing the same 'values' – which may be positive or negative. The use of this system is potentially having huge effects on the behaviours of the local population including acting as an incentive to violence, and is also a possible cause of displacement (see Gilman, p.9; see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31). Owing to the lack of vetted and reliable information in the country, the local population makes decisions about its actions based on rumours, fears and word of mouth. The use of mobile phones to spread information that is not only unverified, but can also be manipulated *ad hoc* (for example, showing an old video of a destroyed village and stating that it was just destroyed the day before, therefore increasing the fear and feeling of a continuous attack being perpetrated against one group or another) can further increase the use of non-vetted and non-verified information to make important decisions, like fleeing from a certain area or looking for weapons to prepare for a potential attack.

Digital networks and security management: understanding information flows or controlling them?

The Central African Republic is not the only example of such systems. In 2014 in Kenya, during the armed attack carried out by Al Shabaab fighters at the popular Westgate mall, several messages were circulated via the WhatsApp smart phone application. One of the messages said,

> An intel guy, who is communicating with a military consultant, who is inside Westgate as we speak says that the terrorists are in Barclays Premier with some hostages and shielded by the bullet proof glass. Other hostages are tied to the pillars in the basement with explosives. Suicide bombers have been dispatched to other four unknown locations. Also confirmed that Samantha Lethwaite is the leader.

Another message was also sent over mobile phones,

> Guys, if you know anyone near that area please tell them to move as far as possible! Apparently all of the third and fourth floor are laced with explosives and those guys may blow anytime. Hear there are over a 100 people dead in Nakumatt maybe all or some of the hostages. They are in Nakumatt basement. All hostages surrounded by bombs. So if anyone tries to do anything they will blow it. So they are planning on how to go about it. Message from Special Squad.

Of course none of this information ended up being true or was ever confirmed by the local authorities. However, those messages helped in spreading panic and rumours and fostered an environment of fear and suspicion within the local population. Anecdotal evidence shows that people indeed left their houses and some even the country for fear of possible other attacks or for fear that the Westgate mall might explode. More research is necessary to determine whether any of those actions were indeed caused by the spread of this information over mobile phones (see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31).

The messages spread over the WhatsApp application in Kenya have several characteristics in common:

1. The explicit request not to spread the information via social media. This made it impossible to correct, deny or confirm any of the rumours.[49]

2. All messages claim to come from an inside source from the official security apparatus.

3. They were all spread using a closed and existing network, WhatsApp, which is based on personal phone numbers. This means that the messages where spread quickly between people that trusted and knew each other well.

These closed systems, like the one used in CAR, spread quickly and work efficiently because they offer many advantages:

1. They are closed systems and rely on peer to peer trust – I trust you and therefore I trust what you are telling me – which allows for the primary source to become irrelevant to the reliability of the information, because the trust is transferred to others.

[49] The capacity of Twitter to generate corrections to rumours was analysed in detail by the London School of Economics following the London riots in 2011. This research found that the power of Twitter users to correct false information was equal to their power to spread it: most rumours were identified as false and corrected within 2-3 hours. See Richards, J. and Lewis, P. (2011). How Twitter was used to spread – and knock down – rumours during the riots. *The Guardian*. 7 Dec. Available from: http://www.theguardian.com/uk/2011/dec/07/how-twitter-spread-rumours-riots. [Accessed 1 Sept. 2014].

2. They allow for the information to spread fast because it is free and relies on homophily; both the Bluetooth and the WhatsApp systems are relatively cheap if not totally free.
3. They prevent any sort of cross-verification from happening. Only people that are inclined to trust the information will receive it and they only share it with others that have their same values, so the likelihood of someone within the system to doubt the information declines considerably.

What these two examples highlight is that technology is not only democratising information but is also sequestering it, confining it into small areas that external actors cannot reach easily, and thereby enabling the creation of more closed systems, rather than open ones. Those systems are based on the existence of confirmation bias, a cognitive stance that favours information that confirms previously existing beliefs.

One of the main differences between the system developed in CAR and the one used in Kenya stems from distinction in the technology used. Systems like WhatsApp, as well as BBM, Twitter and Facebook private conversations, can be monitored by the authorities because they rely on a controlled and accessible infrastructure – the mobile and internet network. Collaborative efforts between authorities and mobile providers have already happened in several cases, such as the London Riots of 2011.[50] On the other hand, systems like Bluetooth are much more difficult to tap into and to monitor because the only way to see what is being exchanged is to have access physically to the phone or to be close enough to the exchange point to tap into it.

The evidence available to date, however, suggests that the approach of controlling or even blocking instant messaging systems has not generated particularly positive effects. Anecdotal evidence on the ground highlights that when a system is not available anymore, people find an alternative to exchange information anyway. No study so far has been able to prove that there are possible beneficial effects deriving from blocking the use of certain technologies. In addition to this, concerns need to be raised in terms of the implications that those types of measures, including surveillance, have when it comes to the right to privacy and to free speech.

There is also a value in being able to understand and see those conversations, and in engaging with the people who take part in them. From a programming and peacebuilding perspective, one of the main possibilities is the opportunity to break the homophily system by inserting voices in the conversation that can bring different and also opposing opinions. From a security perspective there is also a value, albeit an indirect one. As described above, the veracity of the information shared through such networks is often beside the point: therefore, accessing networks of this type is not likely to provide reliable warning of attacks or planned violence *per se*. However, developing ways to track information moving in closed communication systems could provide important insights into the perceptions of conflict and the framework through which parties to conflict interpret events and view those involved (see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31).

One very interesting example of a completely different strategy that leveraged homophily and learnt from violent actors for the creation of a peace-keeping and early warning system is a small project implemented in Kenya during the 2013 elections. Sisi Ni Amani,[51] a local organisation, used mobile phones and SMS as a way to intervene in the decision-making processes that led to violence by studying the triggering factors of violence in different contexts. Sisi Ni Amani was able to use existing networks on the ground to develop a strategy that was based on groups' ethnic and demographic affinities. The messages developed and sent by SMS to people identified as vulnerable to violent behaviour were developed and designed by their peers, and therefore built on their common values and confirmation bias.

More applied research in this field is needed. Most of all, however, there is a need to move beyond the above-mentioned dichotomy: technology, along with other tools, can and will be used in positive and negative ways by affected populations. Preventing or blocking the use of certain technologies will not really address the issue. A much deeper understanding of the dynamics of information in conflict and how internal communication flows can be used to increase exposure to 'the other' and opposing views, rather than increase polarisation, is critically needed.

[50] Jamieson, D. (2011). London Riots Co-ordinated with BlackBerry Messenger. *TechWeek Europe*. 8 Aug. Available from: http://www.techweekeurope.co.uk/news/london-looting-co-ordinated-with-blackberry-messenger-36303. [Accessed 1 Sept. 2014]. Halliday, J. (2011). London riots: BlackBerry to help police probe Messenger looting 'role'. *The Guardian*. 8 Aug. Available from: http://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting. [Accessed 1 Sept. 2014].

[51] http://www.sisiniamani.org. [Accessed 1 Sept. 2014].

Network analysis, which analyses the relationships and interdependency between interacting units (such as individuals) and is widely used in epidemiology, social anthropology and organisational behaviour, has been used to examine and interpret the dynamics of wars for many years.[52] It has also more recently been applied to understanding how the internet functions, and the same approach – looking at how social networks connect and unite social groups – can be applied to offline systems such as mobile. Moody (2005)[53] suggests that a comprehensive social network analysis can help in identifying the magnitude of social multiplier effects, for example.

We also need to start learning from the use of technology by violent actors. Studying and understanding how already existing systems work can help us understand what they rely on, and leverage this information to create positive counter-systems, much like what Sisi Ni Amani did in Kenya. There is a requirement to look carefully at what is happening on the ground from a more sociological point of view, rather than a security one: in humanitarian emergencies local staff are also affected population, and can offer humanitarian organisations a window into the dynamics and tools used by the local population to communicate.

From a security perspective, it is easy to dismiss the kind of information that moves through closed networks: much of it is clearly (deliberately or accidentally) untrue, or (deliberately or accidentally) misrepresentative of ground realities. Yet the available evidence to date suggests that dismissing this information would be wrong. Such information can be extremely useful in predicting humanitarian problems, such as displacement (in response to rumours or threats), identifying misperceptions (deliberate or accidental) regarding the actions of international agencies, and in understanding the drivers of conflict. Accessing and triangulating this information, however, remains a key challenge.

[52] See the work of Emile M. Hafner-Burton, Alexander Montgomery and others.
[53] Moody, J. (2005). Fighting a Hydra: A Note on the Network Embeddedness of the War on Terror. *Structure and Dynamics*. 1 (2). Available from: http://escholarship.org/uc/item/7x3881bs. [Accessed 1 Sept. 2014].

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 66 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

Editors

Raquel Vazquez Llorente and Imogen Wall.

The editors welcome comments and further submissions for future publications or the web-based project. If you are interested in contributing, please email eisf-research@eisf.eu. Imogen Wall can be contacted at imogenwall@hotmail.com.

Acknowledgments

The editors would like to thank Lisa Reilly, EISF Coordinator, for her input and advice, and especially for her comments on the initial drafts. We would also like to extend our gratitude to Tess Dury, for her research support at the initial stages of the project, Brian Shorten for sharing his expertise with us, and Crofton Black for his early guidance and, as always, his continuous support.

Suggested citation

Vazquez Llorente R. and Wall, I. (eds.) (2014) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management*. European Interagency Security Forum (EISF).

Cover photo: Mary Kiperus, community health worker, uses a mobile phone for reporting to the local nurse. Leparua village, Isiolo County, Kenya. February, 2014. © Christian Aid/Elizabeth Dalziel.

Available at
www.eisf.eu

Other EISF Publications

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

Briefing Papers

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Reports

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez, R. (Sp. and Fr.) – EISF Secretariat

Managing The Message: Communication and Media Management in a Crisis
September 2013
Davidson, S., and French, E., EISF Secretariat (eds.)

Family First: Liaison and Support During a Crisis
February 2013 *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L.
– EISF Secretariat

Forthcoming publications

Office Opening Guide