

On Building Trust With Technology

Dr. Ingrid Nyborg, Norwegian University of Life Science
Dr. Bahadar Nawab, COMSATS Institute of Information Technology

Information and communications technologies (ICTs) are quickly becoming an important aspect of post-conflict police reform programs. There is consequently an urgent need to be clear on the purposes of ICTs in police reform and on what expectations the police as well as communities have to the role of ICTs in building secure societies.

Despite this, there is little work done on purposes, roles and expectations, and on how ICTs in fact contribute in reform processes.

Based on fieldwork in Afghanistan and Pakistan, this Policy Brief Concept Note offers insights into these complex challenges from South Asia.



As armed conflicts end, and peacebuilding begins, police reform becomes one of the pillars of international support. For years, this has meant a militarization of police forces.

However, building positive relations between the government and its citizenry is important for a more sustainable peace. This includes developing alternative models of policing and it includes finding inclusive means for communications between authorities and communities.

To this end, new information and communications technologies emerge as important in post-conflict police reform. Such technologies contribute to criminal investigation, crime reporting and administrative capacity. On an expanded view, emerging technologies may also improve trust between citizens and police authorities, thus increasing human security.

ICTs for Fighting Crime

ICTs in police reform are normally used for improving administration within police departments, and for investigation and response to crime. To enhance abilities within crime fighting, modern technologies are adopted to strengthen communications within police departments and for statistical purposes. Cyber forensics to combat data crimes necessitate sophisticated criminal investigation methods, including sophisticated technologies. Another crucial reason for adopting ICTs is the need for informants in crime fighting.

Meanwhile, such technologies also have a role in crime reporting and for emergency services, but they are seen as tools to be used mainly by the police. The benefits and constraints of developing ICTs, therefore, are evaluated in terms of technical capacity, infrastructure, and human skills, and in terms of the capacity of the police themselves, rather than as tools for contributing to human security in conflict-ridden societies.

Fighting crime is thus the prevalent objective of adopting ICTs in post-conflict police reform. Improving relations with communities or contributing to a broader understanding of human security is not necessarily a top priority.

“Fighting crime is the prevalent objective of adopting ICTs in police reform.”

A Perspective on Human Insecurities

Emerging and new technologies as part of security sector reform in post-conflict societies may however contribute to reduce human insecurities and strengthen relations between the general population and the official security apparatus.

To achieve this, what is needed is a broader perspective and a deep understanding of what constitutes human insecurity, and how this can, for example, lead to crime prevention.

Why is this important? Because if there is poor trust in the police, and poor communications between populations and the police, the police are not accountable to the populations they serve. The introduction of ICTs controlled by an unaccountable police could instead threaten the security of members of communities. An expanded view would therefore consider the role of ICTs in improving trust, communication and human security in communities tired of conflict.

Since human security involves the multitude of insecurities experienced by different people in different contexts, ICTs can take many forms and are not reserved exclusively for the use of the police. In fact, ICTs in police reform need not be run by the police themselves, but could involve linking with civil society actors to better communications between the police, communities and community institutions and organizations.

Afghanistan: Misconduct Call Number

In Afghanistan, one of the technologies implemented on the part of the police is a call number originally intended to be used to report police misconduct and corruption. Its use has expanded, however, to crime and emergency reporting. The system was funded by the international community and the technical development provided by a private technology company. The Afghan National Police have built up their capacity to receive calls, and are working on improving response.

“One challenge identified is whether information received and forwarded actually reach the correct office.”

One challenge identified in our preliminary research on the call number is whether information received and forwarded actually reach the correct office sufficiently fast or protects the identity of the caller. This could represent a serious defect in a system that was developed and delivered, but not sufficiently tested under local conditions, and with no provisions made for maintenance. There are currently no funds nor expertise within the police for improving the system. Other shortcomings, such as insufficient knowledge transfer and the lack of a proper messaging system, were also identified.

The call number is nevertheless being tested in several Afghan provinces, but it only covers urban contexts, and the calls are not free of charge. To improve the system while it is being implemented in more regions of the country, the importance of protecting the identity of the caller, con-

trolling who has access to data, and ensuring that it is not used by informants to oppress the population, must not be neglected, as this would result in a decrease in communication and trust between the police and communities.

At the same time, a vibrant ICT civil society community emerging in Kabul is trying to find creative ways to use ICTs to report harassment and corruption, and to improve government services in general. The same issues of balancing reporting with protection of rights and identity, and the issue of trust, have also surfaced in this community. Inclusion of the police in such discussions could prove useful in finding common ground.

“A vibrant ICT civil society in Kabul is trying to find creative ways to use

Pakistan: Push and Pull ICTs

Across the border to Pakistan, a plethora of ICTs is employed to improve policing. Some of these are specifically designed to strengthen the capabilities of the police in criminal investigation, while others have at the core the purpose of strengthening police-community communications.

Cases in point of the former include an Identity Verification System (IVS) and a Vehicle Verification System (VVS) in the Khyber Pakhtunkhwa province.

With the IVS program the police use tablets to verify that personal identity cards match the persons holding them. The objective is to curb the use of fake identity cards, which is common among criminals and militants. The system includes, for instance, data of all legal Afghan refugees in Pakistan. Previously, the police had no system to verify the authenticity of illegal and legal Afghan refugees. With this sort of data stored in the IVS, police teams can easily verify the credentials of anyone who claims to be an Afghan refugee and every click on this system is recorded and monitored in the Central Police Office.

The VVS, which links vehicle records and police officers' mobile phones, was established to reduce the use of stolen cars or fake number plates. The proliferate use of stolen vehicles or fake number plates by terrorists, militants and criminals made it difficult for investigation officers to trace them. The police also observed that most routine stop-and-search exercises were meaningless due to lack of available information. The VVS ensures that complete and authentic details of all vehicles are now available to the police through just an SMS.

With this in mind it is important to appreciate that the by far most visible and interactive face of government authority in Pakistan is the police. With methods such as IVS, VVS and similar in place, the police have under its command

technologies that may be widely susceptible to abuse.

However, included among ICTs in use by the police are also systems that are purpose-built for human security. Among these are, for instance, an Android-based one-click SOS alert service for vulnerable and sensitive institutions, including all schools, in Peshawar. The one-click system sends a signal to the ten closest police stations, and by showing the type of institution, number of students and easiest route to the institution, the police can rapidly reach a school or a college where they are urgently needed.

“The system is put in place to reduce the police-public trust deficit.

Similarly, the Police Access System, also in Khyber Pakhtunkhwa, is established to increase public accessibility and provide swift, prompt and reliable systems of redressal of public complaints. This 24-hour service receives public complaints through telephone, SMS, email, FAX, post, in person and through a toll free helpline. By combining multiple communications channels and platforms, the 24-hour service allows community members to submit complaints using ICTs they currently have access to and use. The system is put in place to reduce what is widely considered a police-public trust deficit.

What all this signals is that in the Afghan border areas of northern Pakistan, a comprehensive system of pull and push ICT methods are being tested and used as means for enhanced police efficiency as well as for stronger and more reliable police-community relations.

Exactly where the emphasis is or ought to be, depends to a large degree on the objective of the ICT system itself. When citizens can attach, in one of the ICT systems implemented in Khyber Pakhtunkhwa, geo-tagged multimedia content, such as photo, audio, and video to support their complaints, the result is both enhanced police efficiency and more reliable police-community relations.

Trust Through Inclusive Technologies?

What this also signals is that in the two South Asia countries under scrutiny here, the contribution of ICTs in improving police-community relations and preventing crime, while also fighting crime and other insecurities, may be immense.

This should not, however, replace other forms of communication. Rather, new technologies, including social media, SMS and apps, may be combined with and enhance more conventional forms of communication and media such as radio, TV, and face-to-face encounters. Ensuring that this perspective is brought into security sector reform is imperative given that new technologies already are part and parcel of any post-conflict reform process.

For new technologies run by the police, there must be close collaboration with civil society and enough technical competence in the police to be able not only to use them, but to adjust them when necessary. This becomes an area of challenge when competence is purchased only for ICT development, and not for testing and maintenance, such as was the case in Afghanistan.

Moreover, criteria need to be developed to assist police reform in defining their specific ICT requirements in ways that link closely with the concerns of civil society and the general population. This should enable better use of existing ICTs that are fit for purpose or the development of new, innovative forms of ICTs which contribute to better forms of communication, mutual trust and accountability

Key Points

- *ICTs for trust-building are not ICTs for surveillance – these are two separate issues.*
- *Police should involve different members of communities in identifying insecurities, and together identify areas of and reasons for distrust.*
- *Promote flexibility and innovativeness on both the police and civilian side in building trust – challenge conventional roles and responsibilities.*
- *Prioritize the development of police skills in communication and consultation with communities.*
- *Invite civil society to participate in development of ICTs for police, and link with civil society developing ICTs for ensuring human security.*
- *Be clear on not only the potential of ICTs, but also the risk to those participating in these types of communications.*
- *Consider the protection of the identity of those using ICTs a top priority: Develop clear policies on who has access to data generated through ICTs, and how this data is used, to ensure integrity and accountability.*

THE PROJECT

The ICT4COP research project seeks to understand human security in post-conflict settings by researching community-based policing and post-conflict police reform.

The Norwegian University of Life Sciences is the project coordinator.

Contact: Frode Bjerås, Research Communications Specialist:
frode.bjerkas@nmbu.no; +4767231384

THE AUTHORS

Dr. Ingrid Nyborg is project leader of ICT4COP, heads up the South Asia and Gender research areas of the project, and Associate Professor at the Department of International Environment and Development Studies, Noragric, Norwegian University of Life Sciences.

Dr. Bahadar Nawab is a member of the South Asia work package of ICT4COP and Associate Professor and Head of Department of Development Studies at COMSATS Institute of Information Technology Abbottabad, Pakistan.



ICT4COP has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 653909