Employing Mobile Applications for Capability Enhancement

TS BAINS

Fire is both a friend and a foe depending on how one uses it. Today, technology is becoming akin to fire. While the world is busy finding ways and means to exploit technology for gainful means, technology is also becoming a tool for terrorists, enemy nations and rogue elements to easily target governments, establishments and people. One is aware of the huge explosion of mobile applications which is taking place in India and all over the world. This begs the question as to how these can be utilised by the Army for its benefit to achieve capability enhancement. We have to look at the benefits which can accrue through the use of mobile applications (apps) while being wary and safeguarding ourselves from the threats which emanate from adversaries who can use the same platform to target us. A few Armies like the US Army are already using mobile apps for the military. A detailed analysis of the feasibility of employing mobile applications for capability enhancement is in order and a pilot project by the Army can bring out important lessons and chart the way forward for using this form for capability enhancement. This article is a primer in this direction.

Military Capability Enhancement and Mobile Apps

Military capability enhancement is a continuous process which militaries have to undergo to remain relevant and operationally effective to be able to achieve strategic, operational and tactical objectives. In the military context, capabilities

Mobile apps can provide high end results in capability enhancement at lower costs

may be analysed in terms of force structure and the preparedness of elements or groupings within that force structure. Capabilities can also be assessed in terms of readiness, training, operational art, sustainability, etc. Due to the advent of technology today, net-centric operations and related concepts are playing an increasingly important role in driving military transformation, and contemporary capability management needs to take cognisance of these factors. While force structures and military hardware may form the bedrock of a nations' military capabilities, the cutting edge is being provided by the skilful use of technology. Thus, technology will play a key role in any nation's quest for national security.

As technologies change, the military has to adapt to these changes and use technologies to its advantage. Technologies like drones, robotics, big data, etc are already making a difference in the Army today. Mobile apps is another area which which can give high end results in capability enhancement at much lower costs. The world over, the smart phone revolution has brought the effectiveness and popularity of mobile apps to the fore. Mobile apps provide easy and immediate access to users thereby increasing efficiency and effectiveness, a key requirement during war. However, in the context of military users, security is a key issue and needs to be paramount while exploiting mobile apps. Military capability enhancement and mobile apps comprise a natural fit and should be exploited.

Mobile Apps Ecosystem

To ensure that creation of mobile apps is not a one-off event, it is essential that the whole mobile apps ecosystem is created so that the required mobile apps are created on a regular basis, old ones are updated and mobile apps support is provided. It would not be possible for an existing institution to take on the additional load of becoming a mobile apps creator. A new institution backed architecture will bear better fruit if the full potential of exploiting mobile apps for military capability enhancement has to be exploited. In the Indian context, a pilot project by a Defence Research and Development Organisation (DRDO), suitably incorporating Army Headquarters (HQ) and HQ ARTRAC and civilian companies should be the pathfinder which can be followed by the formal creation of the organisation. For example, the Defence Advanced Research Projects Agency's (DARPA's) Transformative Apps Programme is one such initiative taken by the US government.

How does one go about building a mobile apps ecosystem? As per Basole, there are four distinct phases for mobile transformation. These are mobilisation, enhancement, reshapement and redefinition.

- **Mobilisation:** The first step in this process is the mobilisation of existing data, applications, and processes. It implies making military data, processes and applications available for use on mobile and wireless devices. The aim is to provide end-users with a new level of convenience by enabling access to context-relevant information, anywhere and at any time.
- **Enhancement:** The next step is to improve existing processes and applications for enhancing and creating new data, applications and processes that leverage the unique functionalities and capabilities of mobile technologies. These typically appear in the form of value-added services; as end-users continue to use mobile applications, new services and flow of information emerge. This will lead to better efficiencies and further capability enhancement.
- **Reshapement:** In this stage, mobile solutions begin to reshape business models and strategies. For the armed forces, this would be the phase in which innovative mobile applications will start aiding in gaining an edge over the adversaries e.g. in terms of shortening the time decision loop, faster reconfiguring of forces, better logistical solutions, etc.
- **Redefinition:** In this final step of the transformation process, mobile solutions create new core competencies.

How will the building of the mobile apps ecosystem evolve in our context? The above steps can provide the initial direction for us to field the mobile apps ecosystem. As mobile infrastructure in Army networks is limited, the mobilisation step in our case would primarily be of mobilising unclassified data, applications and processes which can ride on the civil mobile network. In the enhancement phase, new green field applications with the requisite security overlay can be started on Army networks in addition to the civil mobile networks. The reshapement and redefinition phases of building the ecosystem will finally bring to the fore the full potential of using mobile apps for military capability enhancement. The users, ranging from commanders right down to the lowest echelon of the Army, will be able to use the mobile apps efficiently and be able to exploit them for success in war.

To start with, we may have to look at using mobile apps in two networks. The first is the existing civil mobile network where unclassified mobile apps of utility can be hosted. The second is on the Army network. For the Army network, incorporation of the same will have to be done in the upcoming Tactical

Communication System (TCS). The mobile handsets which will be provided in the TCS will have to be mobile apps compatible. The ability to use the two networks has the following advantages/disadvantages

Indian Army's future network architecture will have to be mobile app compatible

- Unclassified apps can be provided on the civil mobile network. This will increase accessibility.
- The civil network enables the Army to bring into its fold family members of armed forces personnel and civilians who are engaged with the Army.
- Security related mobile apps can be hosted on the Army's own network.
- The organisation making mobile apps will have to deal with two different operating systems as the Army is likely to have its own operating system on the mobile network of TCS.

One could question the need to have mobile apps in two networks. The current mobile architecture in the civil and its differential with the Army network is the main reason for having mobile apps on two networks. The same is amplified as under:

- Mobile apps have achieved acceptability in the civil networks. It is, therefore, easier to roll out mobile apps in the civil networks.
- Rolling out mobile apps on the civil network will give valuable experience which, after integrating the security requirements, can be fielded on our own networks.
- It is easier to sub-contract unclassified mobile apps to a civil agency so as to initiate the process of adapting to the use of mobile apps more effectively for capability enhancement.
- The hardware and software in the armed forces is generally a generation behind the commercial civil networks. We are not in a position to roll out mobile apps on the Army network today. As the generation gap will continue, there would be a requirement to have a separate set of mobile apps.
- As the Tactical Communication System topology and network architecture evolves, the ultimate aim will be to enable the lowest echelons of the Army to access mobile apps. This will take some time and it would be prudent to go ahead with a pilot project of mobile apps based on the civil network.

Pro and Cons of Using Mobile Apps

The pros and cons of any new technology can be compared to fire. If we master technology, the technology will serve us well; however, if we let it make us its slave, then we run the risk of a major security challenge. First, let us look at some examples where mobile apps can lead to capability enhancement.

- **The Indian Global Positioning System (GPS)-Based Compass:** Once our own GPS-based system is in place, it would be easy to launch GPS-based location applications which can function as a compass, give us our location and other related information.
- **Improved Situational Awareness:** Integrating mobile apps with the network will give commanders vastly improved situational awareness. This itself can be a game changer during battle.
- **Decision Matrix Formulation:** It is possible to make decision matrix applications which will aid commanders in decision-making, though the final decision and responsibility rests on their shoulders.
- **Monitoring Systems:** We have a large number of network applications which will be hosted on our own Army network. For example, logistic movement can be easily managed using mobile apps.
- **Training Manuals:** After a review of security classification of our training manuals, unclassified training manuals can be made accessible to our armed forces personnel even in the open domain.
- **A Sea of Apps:** Easily available mobile apps can be adapted to meet our requirements. Health apps linked to our health standards, physical activity apps linked to our physical standards are two such examples. Actually, there is a variety of apps which can be suitably adapted to meet the requirements of the Army.

Undoubtedly, every time a new form of technology comes in, it leads to a certain amount of disruption and turmoil. Like any other technology, mobile apps also come with their share of advantages and disadvantages.

Using Army specific mobile apps will lead to the undermentioned advantages:

- Easier and faster access to information.
- Faster information-based decisions by leaders and commanders.
- Easier dissemination of training.
- Incorporation of military apps of value.
- Easier maintenance.
- Easier and efficient decision support systems.

Security is of paramount importance to the armed forces, but it is a disadvantage where we need to pay special attention, as security hazards should not overwhelm the distinct advantages of mobile apps in the Army. For example, the use of smart phones by all ranks of the Army and their families is on an exponential rise. While smart phones are bringing in benefits to all ranks and

their families, these smart phones also act as a serious security risk as the data of armed forces personnel can be accessed and monitored by malware infected apps. Some apps may be delivered as free apps but would have malware which may seriously affect security. Some of the threats/risks are elaborated below.

- **Location:** Most smart phones have GPS features. Thus, photos taken with geo-tagging can give away the location and sensitive information, especially in operational areas and during war. Use of smart phones will have to be restricted in these areas.
- **Malware:** Inimical elements will try and load malware on the phones of Army personnel through free apps downloads/other means to be able to extract sensitive/classified information on these phones. Both active and passive cyber attacks can be carried out on these phones.
- **Loss of Data:** If a particular phone has been targeted and the phone is hosting classified information, there is an existential risk of loss of data.
- **Hosting Classified Data:** The mobile apps will have to be created in such a manner that they themselves don't host classified data for access by users which can be accessed by inimical forces.

Conclusion

In the coming years, technology will to play a decisive role during both war and peace. Its correct and continuous employment will yield exponential returns. Mobile apps offer a unique opportunity for military capability enhancement at lower cost while offering multiple benefits. Our prowess in the Information Technology (IT) sector means that this can be achieved "in house" in India and we need not be reliant on foreign nations for any technology transfer/import. To fully exploit the capability of mobile apps, there is a need for the Army to start building the ecosystems required to take this forward.

Col **TS Bains** is a Senior Fellow at CLAWS. The views expressed are personal.

References

Rahul C. Basole, "Transforming Enterprises Through Mobile Applications: A Multi-Phase Framework," http://www.ti.gatech.edu/basole/docs/amcis05.pdf

https://en.wikipedia.org/wiki/Capability_management

http://www.militaryaerospace.com/articles/2013/04/DARPA-Transformative-Apps.html