Smart Counter Insurgency: Integration of Technology in Operations

By: [*i]Marjuka Binte Afzal

Keywords: Counter Insurgency, Social Media, Drones, Sensors, Social Media, PSYOPs.

Like all operations, the landscape of counter-insurgency is changing and evolving. With the advanced nature of information and communication technology and globalisation, the world is becoming more and more proactive in its way of arming itself for adversity, and so are the factors from which we pose threat from. Insurgencies and terrorism, as well as transnational organised crimes and syndicates are now weaponised, with social media and the internet, and advanced technology and arms. It is significant to be well-aware of these advances and use the same techniques to build a better countermeasure against these insecurities and threats. To enhance capacity and effectiveness of law enforcement agencies and military forces, it is imperative that we integrate technology in the operations. For the concern of counter-insurgency, we will discuss in this article the myriad of ways technology can be integrated with counter-insurgency operations to alleviate the way these operations are planned and executed to get the optimum results. While many studies of insurgency and counterinsurgency emphasise military tactics and terrorist responses, this article hones in on relevant use of technology and scientific innovations and intelligence to show the Smart ways of counter insurgency operations.

What is Smart Counter Insurgency?

At its centre, counter-insurgency (CI) is a battle for government legitimacy in the minds of its people.[ii] When David Galula summarised the insurgent aim in 1963, he said, "If the insurgent manages to dissociate the population from the counterinsurgent, to control it physically, to get its active support, he will win the war because, in the final analysis, the exercise of political power depends on the tacit or explicit agreement of the population or, at worst, on its submissiveness."[iii] One of the principal ways insurgents acquire popular support is by capitalising on the government ineffectiveness. In fact, government illegitimacy is considered by many CI strategists as the "root cause of and the central strategic problem in today's unstable global-security environment."[iv] Counterinsurgents must therefore have as their primary goal the creation of a government that derives legitimacy from its ability to provide effective security, responsive governance and adequate economic development for its population. In fact, in his Inter-agency Counterinsurgency

Framework, Dr. David Kilcullen, the Chief Strategist of the Office of the Coordinator for Counterterrorism of the U.S. State Department in 2006 considers security, political, and economic mission elements to be co-equal "pillars."[v] And here is where smart CI comes into play. Because of the advanced use of technology and globalisation, insurgency has acquired a new tactic of finding legitimacy through gaining public support, whether that be through spread of disinformation through social media or trying to dwarf administration with their show of power using new weapons and technology. These factors can be cancelled out by use of modern technology and intelligence by the government to arm the counter-insurgency forces. In several examples seen throughout the world, whether the use of unmanned vehicles and drones to attack insurgency camps, using tactical teams armed with advanced technology to take down insurgency operations, or effectively taking down insurgent messages on social media, states like Yemen, Afghanistan, Philippines, and many others come to the list.

How drones can be used in CI

By collecting actionable information from the war region, drones play an important role in counter-insurgency. The drone footage will assist government officials to locate the insurgent groups' positions, track the insurgent leaders, and shut down their anti-national activities. In contrast to ground crew and manned aircraft, drones with their higher resolution payloads, multiple zoom-in capability and extended endurance provide ground officials with a better view to differentiate between civilians and combatants. Drones provide the conventional counter-insurgency policy with logistical assistance and assist in avoiding civilian casualties. Drones have come quite useful in counter-insurgency operations, and Yemen comes in that list of examples. The decapitation operations in which drones play a principal role have led to tactical advantages and often stopped particular operations of terrorism, making it a lot easier to deal with the conflicts in Yemen strategically[vi].

Satellite Can Be Used/Integrated in Intelligence Gathering

Combat patrols in a counterinsurgency include raids, ambushes, security, saturation, and satellite patrols. The satellite patrol uses a base unit to control smaller units, or satellites, that leave and return to the base unit. The advantage of this technique is the unpredictability, to the enemy, of the route, size, locations, and the patrol’s overall axis of advance. Satellite patrols are given either an area or an axis of movement. As with all other patrols, they should have a specific task and purpose.

Controlling multiple small satellite patrols is difficult and requires an experienced leader and excellent communications. The US is known for their use of satellite communications (SATCOM) to scope into insurgent territories overseas[vii]. Gathering intelligence and location as well as information about the geographical features of enemy terrain is what makes satellite communication such a powerful attribute that can be added to CI.

How Surveillance Tools Can Be Used in Detecting Explosives In CI

Surveillance on key individuals, organisations, and activities of interest must be identified and preserved. Increased surveillance of sensitive locations, especially government and civilian arms and ammunition sources, must be maintained. This requires the use of sensors and cameras and other electronic monitoring devices to the maximum to ensure that suspicious areas and routes used by insurgents are constantly guarded. RSTA (Reconnaissance, Surveillance and Target Acquisition) and Information, Surveillance and Recognition are tasks that synchronise and incorporate sensors, asset and processing preparation and operation; exploitation; and dissemination networks in order to directly support current and future operations. This is an integrated function for intelligence and operations. Sensory systems installed can detect movements within a wide area and let the users know if anyone is within the targeted vicinity and whether anyone is approaching.

How Social Media Be Used In CI

Psychological Operations (PSYOPs) are a significant asset credited for the success in several Counter Insurgency operations. Social media has come to dominate the world with its instant dissemination of news and the deeply rooted effects on public opinion. But just like any other ways of using social media, one such way is crafting online messages and contents and sending them put as past of PSYOPs. In several cases, this tactic is called Strategic Communications[viii] rather than PSYOPs, since it is an attempt of the government s and decisionmakers to disassociate their work from ‘propaganda’, which are often spread by insurgents. Examples like the “Green Revolution” of 2009 in Iran come to mind, which was triggered through social media posts on Twitter. The aim of PSYOPs is to therefore influence the target audience, each with highly tailored and specified narratives and approaches. Insurgents often use culture and religion as well as political concerns to bring in public support, but the social media can be used as a media for

PSYOPs to negate that narrative with a counternarrative in its place that promote peace and stability.

Counter Insurgency operations in South Asian states especially need a revisiting. There needs to be a call for using smart CI methods to pad the capabilities and effectiveness of such operations so that conflicts are resolved faster. The enhancement and increase of intelligence gathering capacity, due to use of unmanned vehicles, the decrease of casualty and human vulnerability, the increase of explosive capacity, operational enhancement and many more are just the few advancement using AI and modern technology can bring to the table. What needs to be done in context of South Asia? There needs to be more technology acquired, and manpower needs to be trained and skilled. The interface integration is the most important factor here, there cannot be unequal application of technology, there needs to be modernisation and integration on a whole-scale. Countries like India, Pakistan, Nepal, and Sri Lanka have to different extents overcome the first hurdle of technicalities and introduced themselves to the world of Smart CI, but only to limited fields. South Asia needs to have more than just a one-solution-fits-all approach to Smart Ci and needs to be more innovative and optimistic about investing time and energy behind it, acquiring training and equipment and creating skilled man-power to execute it, for a more holistic and integrated approach to countering insurgency.

---

[*] Marjuka Binte Afzal is a Research Intern working at Bangladesh Institute of Peace and Security Studies (BIPSS).

[ii] Donley, P. H. (2016). Joint Force Quarterly 81 (2nd Quarter, April 2016) Economic Development in Counterinsurgency: Building a Stable Second Pillar. Retrieved January 10, 2021, from National Defense University Press website: https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-81/Article/702054/economic-development-in-counterinsurgency-building-a-stable-second-pillar/

[iii] David Galula, Counterinsurgency Warfare: Theory and Practice (Westport, CT: Praeger Security International, 2006), 4.

[iv] Eliot Cohen et al., “Principles, Imperatives, and Paradoxes of Counterinsurgency,” Military Review, March–April 2006, 49.

[v] Kilcullen, David (28 September 2006). "Three Pillars of Counterinsurgency" (PDF).

[vi] W. Andrew Terrill, “Drones over Yemen: Weighing Military Benefits and Political Costs,” Parameters 42 no. 4/ 43 no. 1 (Winter/Spring 2013), 17–9, 23.

[vii] U.S. Government. (2009). Counterinsurgency Guide. Retrieved from https://2009 2017.state.gov/documents/organization/119629.pdf

[viii] Kandemir, B., & Brand, A. (2017). Social Media in Operations – a Counter-Terrorism Perspective. Retrieved from https://www.stratcomcoe.org/social-media-operations-counter-terrorism-perspective