No one doubts today that technology is essential to war, critical infrastructure, intelligence gathering and counterintelligence measures, terrorist activities and counter-terrorism, propaganda and information warfare, political and social actions and protests, personal security and privacy of individuals. Beyond this general statement though we must continually adjust our common wisdom as reality moves the goalposts, more often than not completely off the pitch.

Consider some of the recent developments. Though Russia’s cyber attacks on its neighbours' infrastructure are old news, the war in Ukraine keeps bringing novel angles. Air and sea drones are used extensively. Western sanctions cause shortages of electronic components, reducing battlefield efficiency of Russian forces and contributing to their inability to achieve air superiority. Starlink satellites provide Ukraine with alternative civilian and military communication infrastructure.

Technology race in the Middle East is no longer regional. Recently even Albania fell victim to a massive Iranian cyber attack. While Ukraine makes good use of inexpensive Turkish drones Russia has enlisted Iran’s technological help, reportedly paying back in strategic missiles. Technological advances get tightly woven into strategic and even geopolitical considerations.

On the other hand, technology does not displace everything else. The most important lesson from Ukraine is that there is no substitute for boots (and tanks) on the ground. Rockets and artillery damage infrastructure more than cyber attacks, too. Similarly, Western discourse on China's suppression of anti-lockdown protests treats the omnipresent face recognition as essential. It probably helps, especially considering the authorities’ willingness to punish erroneously flagged. However, the old-fashioned network of human informers is quite capable of “lo-tech” action. Just another kind of “boots on the ground”.

Early hopes that analysing vast amounts of data would prove effective in combating terrorism and crime led mostly to disappointment. Indeed, ease of deploying technology at scale may be counterproductive: law-abiding citizens vastly outnumber terrorists, rapists, and child abusers, so even a tiny percentage of false positives will drown *bona fide* detections.

Backlash against wholesale information slurping makes technology companies emphasise end-to-end encryption of users' data. WhatsApp chats are encrypted. Apple recently announced iCloud data encryption and backtracked on plans to "make the world safer" by scanning everyone's iPhones for child porn. Safeguarding society's core values rightly trumps law enforcement efficiency.

Nothing here suggests that technology is ineffective. Rather, the argument is that its integration must be approached with more sophistication and subtlety. Neither "tanks are no longer relevant" nor "let's use AI to catch terrorists" cuts it. Policies and actions must adjust to open options and balance benefits against risks. This issue highlights the complexity.

Alessia Maira analyses technology's strategic impact directly. Annalisa Guarise looks at cyber in the military. Antonella Benedetto weighs biometric surveillance in counterterrorism against privacy protection. Ho Ting Hung evaluates the role of technology in the confrontation between China and Taiwan. Rita Sasso addresses ways to counter Jihadi propaganda on social networks. Valeria Lymishchenko discusses legal aspects. The journey is just beginning. I look forward to further contributions from these and other scholars, in ITSS Magazine and elsewhere.

Oleg Goldshmidt
Herzliya, Israel
December 12, 2022