

# Technology, Armed Conflict and Terrorism

Sonia Faiz



Islamic Theology of Counter Terrorism

اسلام کے تھیولوجی آف کاؤنٹر ٹیرورازم



## Introduction

Gradually, entire concept of security, nature of violence and conflict has totally been altered. Technological advances have separately elevated concerns about deadly autonomous-weapons and cyber-attacks the weaponization of bots and drones; also, the live streaming of extremist attacks<sup>1</sup>. Thus, at present the top concerns of each state are about how to impede such capabilities like ‘Strategically Sensitive Items’ (SSIs); like Weapon of Mass Destruction (WMD), dual-use technologies as well as conventional-weapons from getting into the reach of number of states around the planet those are apparently well thought-out unreliable and subverting, or the nastiest nightmare of all getting into the hands of malicious actors; like terrorists and militants.

Besides, there has also been noticed an alarming rise in criminal activities; for example, involving ransom-ware and, data hacks. For the intervening time, international-cooperation is seemed to be under strain and dwindling global potential for the preclusion and resolution of violence and conflict in all forms and manifestations are indeed worrisome factors for all of us because these aspects are encouraging criminal and rogue elements more and more. Conflicts however, are likely to be less fatal now and often waged between domestic-groups rather than involving states. Likewise, homicides are becoming more regular in few parts of the world, at the same time gender-based attacks and targets are rising than ever before globally. In short, the long-term impact of rising violence, disputes, issues in diverse forms and manifestations is appearing in guise of brunt; like armed conflicts, limited wars, territorial conflicts, and terrorism; and gradually growing violent approach among youth is nowadays a more widely recognized and bothersome dilemma worldwide.

<sup>1</sup> The gunman live-streamed the attacks in New Zealand, where 51 people died. <https://www.bbc.com/news/technology-48276802>.

So, day by day ever-increasing improvement in technology, innovations in criminal practices, frequent alterations in military-strategies, battle fronts and international protocols; also each day progress in defence-armaments, continuously shifting powers of peace and wars — transforming regional and international hegemonic powers; constantly emerging State and Armed Non State Actors (ANSAs) are very few but significant aspects which are really adding in to trigger the ‘transformation’ of ‘traditional’ nature of security. And this whole phenomenon is giving rise to insurgencies, terrorism, High and Low Intensity Conflicts (LICs), State Actors and ANSAs and innovative crimes as by-product of aforementioned trend unluckily.

### **Impacts of Technology on Security and Armed Conflicts & its Ramifications**

Besides their benefits, technological advancements and globalisation have caused the emergence and expansion of ANSAs including terrorist groups, transnational organised crime-groups, and insurgencies. The encrypted messaging applications like WhatsApp, and internet itself has become popular medium by which ANSAs generally map and execute their activities, also announce their claims. Likewise, it’s not surprising at all that there are several websites which are dedicated for recruiting young people; who may want to join groups such as Al-Qaeda and the Islamic State (IS). Furthermore, technology has aided the spilling-over of armed conflict. Groups such as the IS and Al-Qaeda have efficiently used the internet as well as messaging applications as mean of their ‘safest communication’ in order to establish their further branches and to expand their franchises in all around the world. Bitter truth is rapidly emerging ANSAs who have kept on taking advantages of globalisation recently as well like; smuggling weapons, goods, people, and foreign currencies across borders. For example, Conflict Armament Research (CAR) is an organisation that tracks and identifies the usage and smuggling of ammunition and conventional weapons in armed conflict, it discovered in 2016, that the IS had got its hands-on large stocks of weapons,

via complex web of illegal trade and from Western states<sup>2</sup>. Essentially, the manner by which the international community deals with conflicts, thus accordingly devise plan to enforce security has also gone changed. Progressively more, governments are inclining to hire out a number of their ‘security tasks’ to domestic and foreign security companies for profit generating. The privatisation of military functions although had begun, in the major states like United States (U.S.) and United Kingdom (U.K.) in the decade 1980s so, hence it was not until the Iraq-war (2003) that this exercise came to the forefront. Moreover, by year 2010, the Private Military Companies (PMCs) were not just being utilized for training, logistics, and maintenance but also to protect military-supply convoys and military-bases. That’s why employing of PMCs has been found controversial more than ever before, following the alleged human rights abuses and sponsoring terrorism two renown PMCs in Iraq; the CACI international at Abu-Ghraib Prison<sup>3</sup> and Black-Water worldwide at Nisour-Square<sup>4</sup>.

Undoubtedly, there are numerous technological advancements that are and will essentially alter the nature of security, and may possibly serve as the direct cause of terrorism and off course would tend to be noteworthy levels of conflict in the years to come. More importantly, the hyper-speed of information accessing and processing on the combat-zone, the vie for the electromagnetic spectrum that go along with that trend, the capability to accurately foresee opponent moves through automated ways, and the preamble of “Intelligentized Decision Support Systems” (IDSS), all these features to a near future will be using by selected nations but by only one, those will be carrying the indispensable resources like U.S., Russia, China and handful of others – those will progressively maintain more step-order level edges in military capability. Hence, they will have the facility to put their foot-soldiers and droves of killing

<sup>2</sup> In 2016, however, they produced a compelling piece of research into the IED component parts being used by IS. It revealed that IS is manufacturing ever more sophisticated and devastating suicide bombs and improvised explosives using civilian components from countries around the world. The report showed that most of the equipment, including chemicals, fertilisers, wire and electronics, is being funnelled through Turkey to the group’s territories. The EU-funded group had analysed improvised explosive devices (IED) collected over 20 months on Iraqi and Syrian frontlines to reveal how the so-called Islamic State has been able to amass its arsenal at an unprecedented speed...Further information can be accessed at <https://aoav.org.uk/2016/conflict-armament-research-car/>

<sup>3</sup> More details can be found at <https://www.business-humanrights.org/en/latest-news/abu-ghraib-lawsuits-against-caci-titan-now-1-3/>.

<sup>4</sup> Blackwater Security Contractor Found Guilty, Again, in Deadly 2007 Iraq Shooting...read more about it at <https://www.nytimes.com/2018/12/19/us/politics/blackwater-security-contractor-iraq-shooting.html>.



machines, anywhere they require to be, and when they want to be, securely with the precise resources in place to assist Kinetic Operations (KOs). Obviously, this isn't all about approving **Artificial Intelligence (AI)**<sup>5</sup> and commercial practices – properly modified for the military usage – simply for the sake of just efficiency... rather it's about new trends of winning wars<sup>6</sup> that might not be a Skynet type solution, or even where humans are removed from the loop.

Importantly, the point which needs to be focused is escalating international fear over the expansion of so-called Lethal Autonomous Weapons (LAWs), those could easily spot and take on a specific target without seeking for any human guidance, by this means transferring liability over life and death from Human Moral Systems (HMSs) to Complex Data Systems (CDSs), so it lacking an ethical compass. The United Nation (U.N.) Secretary-General<sup>7</sup> has called for fully LAWs to be proscribed by International Law (IL), as over 30 nations are having these. Taking matters further, hi-tech change is joining in other unintentional ways that will progressively more undermine the suppositions that back both; the conventional and nuclear deterrence which world leaders have relied on for years worldwide, noticeably increasing both strategic and crisis instability.<sup>8</sup> Nuclear-conventional mess,<sup>9</sup> supremacy of the electromagnetic spectrum<sup>10</sup>, the “precision revolution”,<sup>11</sup> and schemes like “mosaic warfare”,<sup>12</sup> will carry on undermining familiar conception of the nature of conflict. After all these, the most rampant contemporary risk is that of ‘cyber-attacks. According to IBM’s X-Force Incident Response and Intelligence Services (IRIS), the numbers of cyber-attacks had gone double in the just first half of year

<sup>5</sup> Artificial intelligence is known as technology capable of “mimicking human brain patterns,” including by learning and making decisions.

<sup>6</sup> Freedberg, Sydney. “Forget The Terminator For Future Army AI: LTG Wesley”, Breaking Defense, Networks & Cyber. Accessed on September 26, 2020. “The ability to decide — (to) synthesize the volume of information that will be available to us (to) make decisions — is the biggest problem we have.

<sup>7</sup> Autonomous weapons that kill must be banned, insists UN chief, <https://news.un.org/en/story/2019/03/1035381>

<sup>8</sup> See Long, Austin and Green, Brendan Rittenhouse, “Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy”, *Journal of Strategic Studies* Vol. 38, Nos 1-2 (December 2014), pp. 38-73; Lieber, Keir A. and Press, Daryl G., “The End of MAD? The Nuclear Dimension of U.S. Primacy,” *International Security* Vol. 30, No. 4 (Spring 2006); Kristensen, Hans M., McKinzie, Matthew, and Postol, Theodore, “How U.S. nuclear force modernization is undermining strategic stability: The burst-height compensating super-fuze,” *Bulletin of Atomic Scientists*.

<sup>9</sup> Acton, James. “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War” *International Security*. Volume 43 | Issue 1 | Summer 2018 p. 56-99. Accessed on September 25, 2020.

<sup>10</sup> Clark, Brian, et al. “Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance”. Center for Strategic and Budgetary Assessments, October 5, 2017. Accessed on September 21, 2020.

<sup>11</sup> Lieber, Keir A. and Press, Daryl G., “The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence,” *International Security* Vol. 41, No. 4 (Spring 2017). Also, Press, Daryl G. “NC3 and Crisis Instability: Growing Dangers in the 21st Century.” Forthcoming publication via Technology for Global Security at [www.tech4gs.org](http://www.tech4gs.org), September 2020.

<sup>12</sup> Defense Advanced Research Projects Agency (DARPA). “DARPA Tiles Together a Vision of Mosaic Warfare: Banking on cost-effective complexity to overwhelm adversaries.” Accessed on September 21, 2020.

2019 in contrast to the second half of year 2018, and most of them were found targeting oil and gas companies, manufacturers, and educational institutes. Notably, the owners of critical and strategic infrastructure are particularly at verge of danger because malicious-actors aim to target nuclear power plants, hospitals, dams and airport control towers. Over hundred cyber incidents<sup>13</sup> with the impending to undermine global peace and security were noticed; these attacks would cause extensive casualties and smash up. The ever-increasingly fatal cyber aspect of warfare and armed conflicts will continue to compel nations to readjust their approaches to ‘global conflict’. The conflict in Ukraine has offered a window into the convergence of these elements<sup>14</sup>. Explicitly violent, categorized by cyber-combat also the shelling of cities, during which many had to lose their lives not merely via bullet, rather by first having been recognized through Social Engineering; means targeted by digital techniques, afterwards eliminated by conventional means.<sup>15</sup> These aforesaid elements of conflict may change and advance to integrate emerging technologies, as well as probably might contribute to terrorism of all kinds and expressions, also regional and global instability more surely.

Despite the fact that terrorism remains widespread usually, its blow has been fading away in recent years. Worldwide, death toll attributed to terrorism has dropped for a fourth consecutive year<sup>16</sup> in year 2019. Terrorist attacks have become less-lethal as governments stepped up with counter-terrorism effort, local and international coordination, and planning to avert and counter Violent Extremism (VE). The Global Terrorism Index (GTI) 2019 shows that since year 2014 death toll due to acts of terrorism have dropped by over 50% as it declined successively from 33,555 to 15,952.<sup>17</sup> However, the GTI-2019 shows the bitter trend about the scope of terrorism, which has increased with number of casualties caused by

<sup>13</sup> This timeline records significant cyber incidents since 2006. We focus on cyber-attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars. <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>.

<sup>14</sup> Ukraine has been the target of a number of cyber-attacks since the conflict started in 2014. In December 2015, more than 225,000 people lost power across Ukraine in an attack, and in December 2016 parts of Kiev experienced another power blackout following a similar attack targeting a Ukrainian utility company. In June 2017, government and business computer systems in Ukraine were hit by the NotPetya cyberattack; the crippling attack, attributed to Russia, spread to computer systems worldwide and caused billions of dollars in damages...More information can be accessed at: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine>.

<sup>15</sup> Brantly, Aaron, and Collins, Liam (Colonel). “A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities”. Association of the United States Army, November 28, 2018. Accessed on September 28, 2019; Collins, Liam (Colonel). “Russia Gives Lessons in Electronic Warfare”. Association of the United States Army. Accessed on September 28, 2019. Also, Brown, Daniel. “Russian-backed separatists are using terrifying text messages to shock adversaries — and it’s changing the face of warfare”. Business Insider, August 14, 2018. Accessed on September 28, 2020.

<sup>16</sup> Global Terrorism Index 2019, Editor’s Pick, Politics & Foreign Affairs, Society by: Dostonbek Bekmirzaev February 14, 2020, can be accessed at <https://impakter.com/global-terrorism-in-continuous-downfall/>.

<sup>17</sup> Global Terrorism Index is released annually by the Institute for Economics & Peace (IEP) and gives extensive data about global terrorism tendencies.



terrorist activities scattering to 71 nations weighing against to the 67 from the prior year<sup>18</sup>. According to GTI- 2019 ‘**conflict has remained the key driver of terrorism**’ as almost 99 per cent of all terrorist-attributed deaths happening in countries those drawn in a violent conflict or either involved with high levels of political-terror. And, the majority of deadly terrorist attacks took place in the Middle East, Sub-Saharan Africa, and North Africa, Iraq, Afghanistan, Somalia, Nigeria, and Syria have borne the heaviest burden. Significantly, countries with high level of economic development, lack of economic opportunity, social alienation, and state involvement in an external conflict are found to be the major drivers of terrorist activity. But, in Western Europe terrorism-related death toll has fallen dramatically<sup>19</sup> in the past few years, although the frequency of incidents has amplified. There has been found a sizeable boost in the number of attacks executed by actors/elements with belief system; carrying far-right, white-nationalist, or anti-Muslim thoughts in both; Western-Europe and North-America in the past two decades. Exclusively, the number of terrorist incidents across these two regions have elevated from 03 in year 2002 to 59 in year 2017<sup>20</sup> with the social media / technology / internet playing a crucial part in the diffusion of xenophobic-speech and provocation to violence. Mr. Steve Killelea, who is founder and executive chairman of Institute of Economics and Peace (IEP), pointed out about his key research findings that, “**IEP’s research finds that conflict<sup>21</sup> and state-sponsored terrorism<sup>22</sup> are the key causes of terrorism**”.<sup>23</sup> All sorts of extremist groups at present contain example-less entrée to the threshold of general public via means of technology; internet, which allows for well-organized and effectual agitation, recruitment, and propaganda, on top of purchase of weapons and free and unregulated money transfers. More critical situation is developing as nowadays both; State and ANSAs can also exploit AI-enabled deep knowledge to construct ‘deep fakes,’ which generate seemingly genuine footage

18 *Ibid.*

19 Global Terrorism Index 2019, Deaths from terrorism halved in the last four years, but the number of countries affected by terrorism is growing. <http://visionofhumanity.org/indexes/terrorism-index/>

20 *Ibid.*

21 A conflict is a clash of interest. The basis of conflict may vary but it is always a part of society. Basis of conflict may be personal, racial, class, caste, political and international.

22 State-sponsored terrorism is government support of violent non-state actors engaged in terrorism. The use of terrorist organizations as proxies in armed conflicts between state actors became more attractive in the mid-20th century as a result of post World War II developments like the increasing costs of traditional warfare and the risk of nuclear war

23 Steve Killelea, Founder and Executive Chairman of IEP, points out that: “IEP’s research finds that conflict and state-sponsored terror are the key causes of terrorism. In 2018, over 95 percent of deaths from terrorism were occurring in countries that were already in conflict. When combined with countries with high levels of political terror the number jumps to over 99 percent. Of the 10 countries most impacted by terrorism\*, all were involved in at least one violent conflict last year.”

<https://impakter.com/global-terrorism-in-continuous-downfall/>

of people interpolating words which they never uttered in reality and this whole emerging scenario have the tendency to fuel propaganda, divisions, humbug and political instability in all around world.

## **Drone-warfare, ANSAs and Terrorism**

Drone technology has been strapped up for military purposes like KOs, since the decade 1960s and has contributed a key part in armed-conflicts ever since Gulf War in year 1991. The Israel and U.S. dominate the defence market for ‘military unmanned aircraft’. China, for the meantime, is the world's number one manufacturer of ‘civilian drones’<sup>24</sup> while Iran has allegedly more part in transmitting quite sophisticated drone technology to several ANSAs, such as the ‘Houthi rebels’ in Yemen. But, primarily the use of armed-drones or Un-manned Aerial Vehicles (UAVs) in targeted-killings has altered the face of battle during renowned ‘War on Terror’ (WOT). Undoubtedly, the drone-strikes are worked as an essential facet of Hard Power (HP);<sup>25</sup> the key military counter-terrorism strategy – predominantly by the U.S<sup>26</sup> with supporters arguing in its favour, as their use makes killing relatively more efficient, and clean, permitting the military to aim at terrorist’s hideouts whilst minimising civilian fatalities. Otherwise, these avers are extremely confronted with huge number of civilian casualties caused by drone attacks in Pakistan, Afghanistan, Libya, Iraq, Yemen, and Nigeria, therefore, use of drones in KOs or armed-conflicts has been remained as strongly disputed throughout on both legal and moral grounds.

It is reported, more than 15,000 civilians were got killed by explosive-weapons in year 2017 only, furthermore of these, 8,932 approximately have been killed in airstrikes<sup>27</sup>. Hence one perspective for using armed drone-strikes is largely looks it as a case of pre-emptive brutality, where the violence committed by the state is not in reprisal or as penalty, although pre-empting violence is taking place

<sup>24</sup> Who Has What: Countries with Armed Drones, *Source: Michael Fitzsimmons / Shutterstock.com*. For more information visit: <https://www.newamerica.org/international-security/reports/world-drones/who-has-what-countries-with-armed-drones/>

<sup>25</sup> Weapons such as Predator and Reaper drones have been used against targets in Syria, Iraq, Libya and Yemen. The MQ-9 Reaper is a larger, heavier and more capable aircraft than the Predator, capable of carrying a significantly larger weapons payload with a much longer range.

<sup>26</sup> More can be read at: <https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1072&context=jil>

<sup>27</sup> For more information plz consult: <https://www.theguardian.com/global-development/2018/jan/08/civilian-deaths-from-airstrikes-almost-double-year> and Human Cost of the Post-9/11 Wars: Lethality and the Need for Transparency November 2018 By Neta C. Crawford , accessed at September 20,2020. <https://watson.brown.edu/costsofwar/files/cow/imce/papers/2018/Human%20Costs%20Nov%208%202018%20CoW.pdf>





before it happens. Undoubtedly, drone-strikes leave those targets at absolute risk, with no probability of laying down their arms, that's how entirely bypassing due-process, also providing no chance to present proof. Later, pervasive use of drones in Yemen and Iraq, also the terror it has created in people, had seemed too concurrent to stimulate public anger.<sup>28</sup> Hence it left impression as giving rise to new buds or waves of terrorism with feelings of vengeance and revenge in wake of killings of their loved-ones in armed drone-strikes. On the contrary, from the military point of view or second perspective is about those who are doing the killings are totally risk-free, making out their targets from far-off, with no possibility of physical damage to themselves.

Whilst the third prevailing perspective about relying on armed-drones as 'military-strategy' by any country against anyone also poses solemn questions about understandings of 'sovereignty and war.' It's worth writing drones have been used repeatedly in many countries that are not really 'at war' with those using the drones against them. Likewise, in Pakistan, drone-strikes by the U.S. have been occurring repetitively without approval,<sup>29</sup> led Pakistan to lay blame on the U.S. for infringing its sovereignty. State sovereignty is an imperative worldwide political and official norm, which distinguishes supreme influence of the state within its territorial borders. These instances amongst others, has generated totally different perspective that drone-strikes have to be better considered as a form of **State-terrorism**<sup>30</sup>, by tagging this type of feat as pre-emptive massacre and assassination. State-terrorism is not known as a crime by IL, which can be tied to the historical perceptive that states have a cartel on the use of aggression. Nevertheless, there has been bigger contestation over state sponsored terrorism, manipulated by the global recognition of unalienable human-rights; therefore, changing altogether the concept of how states get legitimacy, and the right of sovereign authority.

<sup>28</sup> From Iraq to Yemen, drones raise U.S. alarm over Iranian plans. By: Babak Dehghanpisheh, Phil Stewart, *Reuters*, accessed at September 30, 2020, <https://www.reuters.com/article/us-mideast-iran-drones-idUSKCN1UC1X4>.

<sup>29</sup> The Drone War in Pakistan, *New America*, accessed at September 2020, <https://www.newamerica.org/international-security/reports/americas-counterterrorism-wars/the-drone-war-in-pakistan/>.

<sup>30</sup> Quite simply, state terrorism is used to describe acts of terrorism perpetrated by a state (rather than a non-state actor or organisation), both against its own citizens and within its territorial limits, and against foreign citizens outside of that state's own territory. State terrorism is different to state-sanctioned terrorism, which can be understood as the support of non-state terrorism by a state.

But with passage of time, drones are becoming ever-more controlling, powerful and smarter, which turns those to be increasingly striking for ‘legitimate’ use, but also for ‘antagonistic’ acts like terrorism. Terrorist-outfits are progressively more employing ‘21<sup>st</sup> century technologies’, including drones and elementary AI in attacks. As these are continuously to be weaponized, AI may perhaps prove to be a dreadful threat, permitting adversaries including ANSAs to mechanize killings on a colossal level. The fatal ‘hotchpotch’ of more sophisticated AI and drone expertise may perhaps allow terrorist-outfits to either attain or develop “LAWs or killer robots,” which would dramatically increase their competence to initiate mass destruction in cities.

As the technology progressed, it has become imperative for high-command or authorities sitting on decision making seats to keep an eye on the risk of both types; as it appears ‘today’ and how it will give the impression of being in the ‘future.’ Drones are ‘increasingly’ more brought by the wrong hands<sup>31</sup> into play for illicit activities Organized Crime Gangs (OCGs) have installed the ‘technology’ to smuggle cigarettes, drugs, and other goods of high value across borders and even into prisons. In year 2016, the IS accomplished its first thriving drone attack in northern Iraq by killing two ‘Peshmerga’ Kurdish warriors.<sup>32</sup> This attack maintained the group’s record of making use of increasingly ‘sophisticated drone technologies’ against its enemies, so this brutal trend later mimicked by other ANSAs universally. The subsequent year, the IS declared the more specialized configuration of the Unmanned Aircraft of the Mujahedeen (UAM) a division<sup>33</sup> devoted to the expansion and use of drones a more formal step regarding the systematic weaponization of drone technology. The abovementioned IS attack was not the first example of ANSAs operating drones in combat, rather an ‘unidentified Syrian rebel group’ in January 2018 positioned a horde<sup>34</sup> of 13 ‘homemade drones’ carrying small submunitions to assault Russian bases at Tartus and Khmeimim, while killing attempt<sup>35</sup> against Venezuela’s Nicolas Maduro exercised

31 Saudi oil attacks: Who’s using drones in the Middle East? By Jonathan Marcus, *BBC*, accessed at September 2020, <https://www.bbc.com/news/world-middle-east-49718828>.

32 Read more about it at <https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says/>.

33 Inside The Chilling World Of Artificially Intelligent Drones, by Volodymyr Goinyk/Shutterstock, ‘*The American Conservative*’ accessed at 30st Sept. 2020, <https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones/>.

34 *Ibid.* ‘Inside The Chilling World Of Artificially Intelligent Drones’

35 Venezuela’s Nicolás Maduro survives apparent assassination attempt, ‘*The Guardian*’, accessed at 29 Sept. 2020, <https://www.theguardian.com/world/2018/aug/04/nicolas-maduros-speech-cut-short-while-soldiers-scatter>.



exploding drones in August 2018. Over and above, the ‘Hezbollah’ which is famous ‘Lebanese’ militant-group is reportedly having the most highly developed ‘drone technology’<sup>36</sup> of any ANSAs. The ‘Houthi’ Iran-backed notorious rebel group have also found using drones to target Saudi Air Defence ‘SAD’ during civil war in Yemen.<sup>37</sup> Other ‘malicious’ use of rogue-drones; included in December 2018, the thirty hour disturbance to flights at ‘Britain's Gatwick Airport’.<sup>38</sup> Later on, Germany's Federal Defence Forces (the Bundeswehr), carried out tests on technology to neutralize threat from intrusive armed-drones to thwart an identical occurrence happening at a ‘German airport’.<sup>39</sup> Subsequently, the amplified threat from armed-drones has prompted more than a few companies to devise technologies that can compel the aircraft for getting out of the aerial space include drones-fitted with nets to catch aberrant vehicles, electronic-fences that jam ‘drone signals’ and hand-held weapons.

## **Conclusion and Recommendations**

No doubt that technology, hi-tech warfare and an increasingly globalised-world has revised the long-established nature of security and now it seems openly interconnected with conflict and terrorism. All the way through history, the evolution of warfare-strategies has depended on the level of technology on hand to warriors / leaders / State and ANSAs. At present, while fundamental human instincts are same, technology has developed the human-capacity to cause smash up and damage. Therefore, nation like human beings, struggle either by elevating themselves to advanced levels of techno-economic development or by bringing others down, technically and economically either by sponsoring proxies or terrorism in hostile states i.e. terrorism which is not a novel occurrence rather it’s becoming significant ‘war strategy’ at present day. However, it’s also fact, ‘terrorism’ on the whole symbolizes a diminutive portion of the ‘global costs’ caused by violence and its equivalent to \$14.1 trillion in year 2018, and herein it diverges from other forms of violence like armed-conflict, homicide and defence expenditure,

<sup>36</sup> Find more about it here, <https://fas.org/wp-content/uploads/2014/06/Hezbollah-Drones-Spring-2014.pdf>

<sup>37</sup> *Ibid.*

<sup>38</sup> Gatwick Airport: Drones ground flights, *BBC*, accessed at September 18, 2020, <https://www.bbc.com/news/uk-england-sussex-46623754>.

<sup>39</sup> Read more about it at, <https://www.dw.com/en/german-military-considers-using-armed-drones/a-53395829>.



according to GTI. Alternatively, the real economic side-effects of terrorism would certainly be larger as this guesstimate does not take into contemplation the indirect consequences and penalties for capital, businesses and spending related to Combating Terrorist Organizations (CTOs).

Technological progress is really adding in varying nature of conflict. Thus, there are apprehensions about the potential for machine-learning and AI to heighten risk of physical, biological and cyber-attacks<sup>40</sup>—like by making them harder to attribute, accurately targeted as well as easier for small independent groups possibly even ‘lone wolfs’ to accomplish. On the flip side, progress in AI and other technological advancement also offer new gears and preventive-strategies for policing, counter-intelligence agencies, and counter-terrorism departments to thwart attacks and recognize perpetrators quickly. Nevertheless, here also are risks involved i.e. predictive policing are associated with its own drawbacks, together with inbuilt-biases; like racial and religious which can stimulate radicalisation to VE. Unquestionably, emerging technologies however is lowering the obstacles to the getting hold of biological weapons other fatal diseases or toxic substances used to impair or kill livestock, crops and humans. Similarly, there is a serious doubt that advances in AI and 3D-printing may perhaps make possible biological attacks with ease by automating the progress and manufacturing of weapons and the malicious-systems that develop them.

The critical analysis of hi-tech-interconnections between security, threat-perceptions and risk management clearly reveals out the important character that technology has been playing in the past and the certainty of its mounting impact in the future as well. Though, technology or the military-hardware produced is in itself only a means to fight back but it being taken as ‘an end’ unfortunately. More to the point, security-planning, military-strategies as well as organizational-infrastructures for putting these counter-strategies into practice is the key to success for establishing peace. It is technology that provides

<sup>40</sup>[https://www.unog.ch/80256EE600585943/\(httpPages\)/29B727532FECBE96C12571860035A6DB?OpenDocument](https://www.unog.ch/80256EE600585943/(httpPages)/29B727532FECBE96C12571860035A6DB?OpenDocument).

military-planners with a range of options like drones, corresponding to the variety of techno-military competences available to counter any threat i.e. war / terrorism / conflicts.

Nearly two decades ago, in year 2001, the first armed-drone had stroked in Afghanistan and in Yemen in year 2002 respectively, made big breaking news. From these isolated horrible attacks, drone-strikes have turned to be regular feature of KOs (Hard Power). Since then, a growing number of both states and ANSAs are applying armed-drones to execute attacks, outside and within zones of armed conflict, with shocking humanitarian crisis at cost of the civilian population hence; drone's debut as a main 'terrorist tool' against the world is very worrisome factor, as ANSAs develop its AI capabilities, the U.N. and world should also reinforce its anti-AI capacity, particularly focusing at ANSAs and the lasting threats they masquerade. In addition, while armed-drones are not explicitly regulated by IL, rather their exercise is administrated by general rules of IL; including international humanitarian law (IHL). These challenges are aggravated when armed-drones carry 'explosive weapons' in populated region. In particular, because of its accuracy, the pay-loads required to demolish the military objective can be decreased and the damage done to civilian population and their belongings may be curtailed. Having written that, this 'precision' depends on the merit of the information gathered from intelligence sources, based on which normally 'targeting decision' is made, which is off course difficult to gather at a distance, but no compromise should be made on its accuracy and authenticity in order to avoid innocent casualties.

Unluckily, elements of regular organized crime and narcotic-trafficking are sharing universal moral fiber with the 'philosophy of terrorism', and this 'nexus' is further supported by immature dictatorial states those are excited to use 'Asymmetric Forces' to clear up scores ahead of their conventional-capabilities. So, therefore, preventing the mishandling of technology for such malevolent purposes will necessitate innovative and joint approaches. Provided that, the probability for regional conflict however, remains elevated; accordingly, likelihood of limited local wars and LICs will also keep on being high, principally

where such conflicts involve dictatorial regimes. Markedly, high-class counter-terrorism choices are inadequate. ANSAs are already setting out drones to hit their enemies. Terrorist-groups will be interested in AI and LAWs for three reasons traceability, cost, and effectiveness. LAWs systems are likely to proliferate to terrorist-groups with potentially shocking consequences. The U.N. and its member's states should right away address the mounting threat by putting in order stronger defences against probable swarm and drone attacks, by engaging with their defence industries and AI experts forewarning of the threat, and opinionated realistic worldwide efforts to proscribe or stigmatize military applications of AI. Even though the chances of such an event are very slight, but the risk is looming, and the time has got nearer to proceed Non-Lethal Weapons (NLWs) and technologies, over and above techno-economic enticements and disincentives are required to play a main role in the management of future armed-conflicts. Endorsing democratic-governance and boosting economic-development in 'troubled regions' can drastically reduce the likelihood of armed-conflict. Nonetheless, if all others fail, subsequently global intervention will be requisite to contain some latent circumstances. The concepts like '**punitive action**'<sup>41</sup> and '**pre-emption**'<sup>42</sup> are positively valuable if exercised with consensus and acumen; even so, it necessitates a careful articulation of these ideas to achieve global recognition, which will affix momentous deterrence value to such counter-measures.

In nutshell, hazards to universal peace and stability have been packed together on two counts;

1. First, the need for a nuclear-balance of terror and impression of guaranteeing national security are being modified to blend both capabilities; defensive and offensive, following end of the cold war; as adapted to the different parts of the world.
2. Second, the use of WMD, or rest of weapons capable of mass-killings, are getting intolerable in progressive, modern, and civil society.

<sup>41</sup> Means any action which may lead to dismissal, demotion, suspension of state as a punishment who fails to fulfil the terms of an agreement; punishment might consist of charge-backs, member-ship cancellation of world organizations, or the threat of trade contract cancellation, reduction in financial aid, loan or economic sanctions etc.

<sup>42</sup> A preemptive war is a war that is commenced in an attempt to repel or defeat a perceived imminent offensive or invasion, or to gain a strategic advantage in an impending (allegedly unavoidable) war shortly before that attack materializes. It is a war that preemptively 'breaks the peace'.



For these aforesaid reasons, the global-taboo on such weaponry and on futile killings in general, perhaps may go en route for reducing ‘terrorization’ of ‘security’ from such armaments and tactics. Future security fears at the universal level will perhaps be more about, resource constraints, health, migration, economic competition and environmental issues. While, common security-concerns are tied to proliferation of hazardous weapons; spreading of terrorism, multiplying of religious-fundamentalism and will entail broader agreement and cooperation. Hence, the new ‘security environment’ may offer an opportunity for all-inclusive cooperation on matters of common distress among responsible and progressive nations. As is frequently said, ‘peace’ is not just the lack of war; likewise, ‘security’ is not just missing of an impending threat. As a result, long-lasting solutions for harmony and security must be footed on ‘globally accepted norms’ that not only are essentially fair, but also seem sustainable on various conditions. Such customs and standards alone can generate the environment for pleasant-sounding relations among majority of international community that require sharing the benefits of ‘peace and security’.

*ITCT does not necessarily endorse any or all views expressed by the author in the article.*