Report 09/04 2019

EGIC
Euro-Gulf Information Centre

CONFERENCE REPORT

Advanced Technologies and Terrorism

Future Threats: Defence and Prevention

by Antonino Occhiuto

On 4 April 2019, the Euro-Gulf Information Centre (EGIC) hosted Professor Darya Bazarkina to further stimulate debate on the issues related to psychological warfare and their importance in the fight against global jihadi terrorism. Professor Bazarkina, teaching and researching at the Department of International Security and Foreign Policy of Russia (Russian Presidential Academy of National Economy and Public Administration) and School of International Relations (Saint Petersburg State University), is an accomplished expert in international cooperation on counter-terrorism, with a special focus on the war of ideas and propaganda. She presented her latest research on the developing relationship between advanced technologies and terrorism.

This comes at the time in which technologies and cyberspace are increasingly important for the transitioning economies of the Arab Gulf. The United Arab Emirates (UAE), has very recently registered its first Crypto-currency Exchange in Dubai. Saudi Arabia, the largest country in the region, is currently committed to the Vision 2030 programme, an ambitious economic diversification plan, in which a key focus will be on new technologies, that aims to reduce and then end Riyadh's dependence on its oil reserves. Bahrain, notably, has invested to create its own FinTech Bay, which is currently the leading FinTech Hub in the Middle East and Africa. In the Gulf, technology already plays an important role to prevent the spread of radical ideologies and track terrorism financing. As

such, understanding the importance of Malicious Use of Advanced Technologies (MUAI) and the various techniques that can be employed to securitise the use of new technologies is crucial to predict some important future challenges that Gulf countries will have to face in the future.

The terrorist threat has long been borderless, and global. Today, even more so, as groups commenced mastering technologies to their benefit. Globalisation is an ongoing and seemingly unstoppable phenomena and, due to the digital revolution, terrorist groups can still survive - and even thrive - in the cybersphere. This was recently demonstrated by the ability of groups such as Daesh and AQAP to use new technologies to organise and carry out terrorist attacks in Europe despite being forced to abandon territories, resources and logistical centres across the Greater Middle East.

Beyond the organisation of specific attacks, advanced technologies have the potential to strongly enhance the impact of psychological warfare (PW), thus providing terrorist groups with yet another instrument in their effort to destabilise societies and create chaos. According to a survey published by the US based Neustar company, 82% of the security experts interviewed currently regard MUAI as the most formidable threat to both private businesses and government functioning. According to Professor Bazarkina, this is due to the fact that MUAI is a diverse and multifaceted threat. For instance, it can take the form of reorientation of commercial AI systems. So called “Deepfakes”, such as fake videos of prominent politicians disseminating hate or fake representation demonstrating popular support for terrorist activities are another example of MUAI. Terrorist organisations might also be able to master predictive algorithms using them as advanced technological weapons to interfere with elections results. What makes MUAI particularly attractive is the fact that to date attacks involving the use of advanced technologies are particularly difficult to predict and it is often very problematic to track down perpetrators. The mix of effectiveness and potential impunity is likely to increase the number of such

attacks in the future.

MUAI can also be used by terrorist groups in more traditional present-day activities. Artificial intelligence programmes which monitor personal internet behaviour, can be used by terrorist recruiters to select the most suitable profiles to be indoctrinated and convinced to carry out a suicide mission. Artificial intelligence could also enable terrorist organisations to claim responsibility for nefarious events which are not related to one another for the purpose of weakening citizens' confidence in state institutions or, more dangerously, turning states against tone another.

The aforementioned considerations lead Professor Bazarkina to recommend a stronger national, regional and international focus to prevent and contrast MUAI, that requires the creation of specialised centres focusing on MUAI in the context of countering terrorism. Authorities should also use predictive analysis extensively to identify potential reasons for social unrest and implement policies to contain them. Despite not being strictly MUAI related, long term programmes enhancing social cohesion are likely to reduce the appeal of terrorist recruiters even if when those are able to increase their outreach via new technologies. Governments should also provide citizens with a better understanding about terrorism's destructive aims and its new tactics.

As the struggle against terrorism carries on, societies and states must ensure they are more capable then terrorists in the use of new advanced technologies. Terrorist propaganda can be submerged online by anti-terrorism content ,while the monitoring of online behaviour, used by terrorist to radicalise, can be undermined by using the same technology to identify radicalised citizens. When it comes to the use of advanced technologies, the largest possible level of international cooperation and expertise sharing are needed to ensure that anti and counter terrorism efforts stay ahead of terrorism.