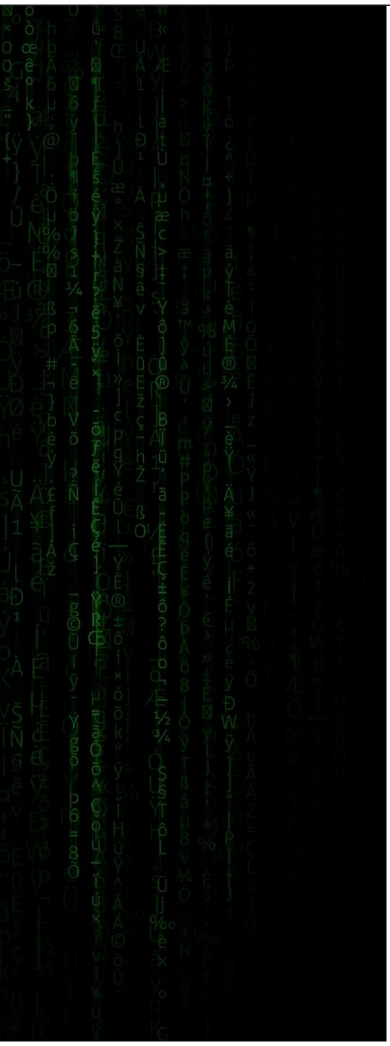
INTERNET EXTREMISM

Paolo Zucconi *examines the world of E-Jihad and reveals how cyberspace assists extremist strategy and tactics*

The nefarious use of the cyber domain helps accomplish Islamic terrorist organisations strategic and tactical aims worldwide. Since 1996, it has been used for jihadi activities. Azzam.com is a perfect example. It is a jihadist website to honor Abdallah Azzam, the mentor of Osama bin Ladin and Ayman al-Zawahiri. Babar Ahmad – an engineering student at Imperial College, London – was accused of being the founder.

Al-Qaeda demonstrated its ability to recruit people and spread its propaganda worldwide through IT instruments. Osama bin Ladin used internet technology in 1997. In 2003 Hezbollah promoted Special Force, a video game simulating terrorist attacks on Israeli targets. Since the nineties, the internet has served as platform for spreading extremist messages. More recent terrorist organisations like the Islamic State (IS) have been able to profit from al-Qaeda's roots in communication strategy. They use cyber capabilities for propaganda, recruitment, communication, training, fundraising and targeting.

Although IT tools are used for several purposes, propaganda and recruitment remain the most relevant. Due to a sophisticated and effective communication strategy that involves IT tools – mostly social networks – extremist propaganda messages can be disseminated worldwide to attract younger generations. The use of social media – Twitter, Facebook, Telegram – is the most important, effective and fastest way to recruit. In 2015, *The New York Times*, quoting American officials, reported that supporters of IS post approximately 90,000 tweets every day.



Most training and information for potential terrorists can be found and spread online via the Dark Web

Although IS has top management and logistic hubs for cyber activities, its current asymmetric feature reflects in the digital world. Recruiters can be anywhere and do not need to be specifically affiliated or trained. They are autonomous, use their own laptops to access social media, get IS propaganda material, and post jihadi messages online.

Recruiters can be both religious and non-religious people, members of IS, of local jihadi groups and even people inspired by jihad but with no official connection to specific organisations. They all merge in the cyberspace, including Dark Web and social media, fueling a large community of potential well-trained terrorists, affiliates and lone wolves.

By posting online extremist public discourses and videos, they recruit in Western countries just like in the Muslim world. This contributes to make the Islamic State an asymmetric entity capable of attracting young people with different backgrounds – poor and well-educated wealthy people alike.

SPREADING THE WORD

As the cyber domain has no borders, propaganda goes beyond and helps IS to turn itself from an Islamic terrorist organisation into a global brand name. It intersects with other local and regional jihadi groups, interested in partnering with international terrorist organisations to gain international attention, image and even logistic support to pursue their attacks.

However, jihadist propaganda and recruitment is more than public discourse. Cinematic videos are posted online – ie IS videos with black flags on the Vatican City or tanks advancing towards the Colosseum in Rome – as psychological warfare techniques to evoke fear.

Terrorist organisations – like Al-Qaeda in the Arabian Peninsula (AQAP) – use educational cartoons and video games to convince children of jihad. According to Professor Raphael Cohen-Almagor (University of Hull) AQAP also publishes an English language jihadist magazine called *Inspire* to radicalise English-speaking Muslims to convince them to engage in militant activity.

The use of online magazines is popular among extremist movements because it helps to defeat the obstacles of distance and language. Al-Shabaab publishes *Gaidi Mtaani*, AQAP *Inspire*, while *Dabiq* and *Rumiyah* are published by the Islamic State. Magazines can be found in several languages in Western countries to attract as many readers as possible. Jihadi forums then provide platforms for networking with other extremists and to fuel radical discourse. People share aspirations and exchange ideas as part of a greater community with shared values.

Websites are also used as online libraries for jihadist literature to provide background to radicalised activists.

The extensive use of social media as well as blogs, video, music, forums, graphic hosting services and other communication apps facilitates reaching a large audience. Jihadist websites compete with each other to get the support of potential followers. But the use of IT instruments for communication purposes is related to the exchange of ideas, shared aspirations and planning attacks. In 2017, Turkish authorities found that Telegram was used to receive information and directions from an IS leader in Raqqa for the New Year's Eve attack in Istanbul. In March 2018, Australia's Minister of Home Affairs, Peter Dutton, reported: "The use of encrypted messaging apps by terrorists and criminals is potentially the most significant degradation of intelligence capability in modern times". This shows that it is difficult for public authorities to fight E-Jihad and propaganda online.

As social media including YouTube, Facebook and Twitter have adopted stricter security measures to counter radicalisation, terrorists have started to use other encrypted chat apps to provide directions for attacks. As encryption increasingly becomes a key part of online messaging apps, Islamist terrorists are exploiting little-known encrypted apps to communicate and provide directions both for attacks and logistic support. This helps them to 'go dark' and makes it difficult for counter-terrorism agencies to track them and intervene.

When it comes to training, some terrorist groups like the Al Nusra Front in Syria and IS continue to use training facilities – basic physical fitness training, weapons training, armed assault techniques. However, they are few and are increasingly proving to be useless.

There are also training camps in Western countries, like the United States. On 13 May, the FBI discovered a two-acre plot of land near Tuskegee, Alabama, linked to a jihadist training camp in New Mexico, where children were trained to commit shootings.

TERRORIST GROUPS MAKE EXTENSIVE USE OF SOCIAL MEDIA TO RECRUIT YOUNGER GENERATIONS

However, most of the training is conducted online. There is free online information and videos serving as instructions and manuals to download from password-protected websites on physical training, bomb making and kidnapping. This helps 'home-grown' terrorists to get trained without going to Syria or conflict zones, teaches them how to 'stay dark' and how to coordinate with other individuals and facilities to assist them in mounting a terrorist attack.

RAISING FUNDS

The internet is also used to get funds by donations and selling of goods. SadaqaCoins is a basic.onion site on the Dark Web that is used to finance jihadist groups, although it is difficult to track this cryptocurrency and know exactly who gets those funds. The Islamic State has financed itself through oil, weapons, drug trafficking, taxation of citizens living in IS territory, and other criminal activities in Syria, Iraq and Libya until its defeat in many regions. Home-grown terrorists and lone-wolves, inspired by extremist propaganda just like other jihadist organisations, get funded through their websites, fraud, gambling or online brokering. Other activities include small donations and funding through charity groups.

However, the most important source of financing is related to the huge amount of money the Islamic State laundered over the last few years into the legitimate economy of the Middle East and beyond. It is estimated IS still has hundreds of millions of dollars.

According to Doctor Hans-Jakob Schindler, Senior Director at the Counter Extremism Project, this requires the adoption of financial counter-terrorism and anti-money laundering measures to prevent IS from continuing to benefit from its crimes. Cutting off terrorism finance is the most effective measure in the war on terror.

The use of the internet for targeting selection is related to the possibility for everyone to easily use open-source programs and intelligence analysis (OSINT) to identify multiple soft targets. By using GPS programs and digital maps it is possible to analyse images and choose potential multiple targets to attack to cause mass casualties, and analyse the area around for escape.

The use of cyberspace by terrorist organisations like the Islamic State has dramatically increased opportunities for extremists to join organisation's activities and therefore recruitment of additional operatives and logistic supporters.

CYBER PROPAGANDA HELPS ISLAMIC STATE TO REBRAND ITSELF INTO A GLOBAL BRAND NAME

Violent terrorist attacks can be highly sophisticated or simply carried out by lone wolves acting to emulate or unable to find appropriate training and logistics to execute attacks. In both cases the cyber domain play a key role.

Terrorist organisations make extensive and effective use of social media to recruit young generations and spread propaganda. The asymmetric component of the Islamic State makes the organisation capable of attracting people everywhere, to attack globally, challenging national counter-terrorism policies.

IT technology helps sophisticated attacks to be pursued effectively as it facilitates quick interactions among the attackers and providers of logistic support. By browsing on open-source programs, specific jihadi websites and the Dark Web it is possible to gather all the information required on potential targets, training, weapons and equipment.

RESISTING POWER POLICIES

E-Jihad is the most dangerous terror threat as it goes beyond borders, while respondees are mostly national. Governments have adopted counter-terrorism policy based on hard power – defeating the IS in Syria and Iraq. But the asymmetric transnational characteristic of the Islamic State and other local organisations has proven resistant to hard power policies.

Also, closing websites and deleting posts has proved to be an understandable but largely ineffective measure. Although social networks have recently adopted measures to counter online radicalism and extremist messages, like deleting posts and violent content, this takes place only after messages have been uploaded and viewed by thousands of people.

Furthermore, many local governments where terrorist groups are based –Niger, Chad, Nigeria, Iraq and Syria – have to face insurgency as well. They cannot devote much money in countering cyber terrorism and do not have appropriate equipment to face online propaganda. Western countries have the resources, but still choose to adopt hard power policies. The use of a counter-narrative could instead facilitate de-radicalisation and avoid cyberspace becoming the major tool for radicalisation and attracting younger generations. As the Islamic State has recently weakened, al-Qaeda could re-establish itself as global jihadist actor and cyberspace can play a crucial role ●

Paolo Zucconi is a Research Associate at the University of St. Andrews Institute of Middle East, Central Asia and Caucasus Studies and Research Fellow at the Global Center for Security Studies. He is an independent geopolitical analyst and Contributor for The Foreign Policy Centre and The Global Policy Journal at Durham University.

Turkish authorities discovered that Telegram was used to communicate instructions from an IS leader for the 2017 New Year's Eve attack in Istanbul

Picture credit: Getty