BRUSSELS
INTERNATIONAL
CENTER

MARCH 2021

New Terrorism and the Use of Electronic Jihad

AVERA – COMMENTARY

By Brahim Laytouss- Head of AVERA Department

1. INTRODUCTION

A new form of terrorism has emerged after the defeat of the Islamic State caliphate in Iraq and Syria in 2019 and the resulting loss of its territory. Under the name of " United Cyber Caliphate " it is trying to find root everywhere in the world, including Europe.

It is important to remind ourselves how IS was able to recruit more than 40,000 Foreign Fighters from 110 different countries in 2013 in the aftermath of the Arabic Spring, many of them believing in a righteous cause, and manage the establishment of a caliphate in large swaths of Syria and Iraq. It is only after seldom before seen atrocities, terror and crimes against humanity became exposed to the world, that an international coalition was mobilized to defeat IS and curb the supposedly " Caliphate ".

However, radical Islam has since then reinvented themselves and adapted a new strategy of cyber-terrorism that will dominate much of the international security landscape in the foreseeable future.

CYBER-TERRORISM HISTORY AND DEFINITION

As we discussed in previous articles, various experts and academics have argued about the exact definition of the what is terrorism. For the purpose of this article we have defined terrorism as "a politically motivated tactic involving the threat or use of force or violence in which the pursuit of the public plays a significant role."[1]

Cyber-terrorism is then the convergence of cyberspace and terrorism. It refers to "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not."[2]

Cyber-threats can be categorized depending on the target (individual, groups or states); objectives (espionage, sabotage, subversion and damage)[3]; the degree and extend of damage (limited, medium or considerable); the type of attack (material, social, political, economic, ideological or religious); and the type of actor (experts, unknown, state actors or organizations).

Today, so-called "electronic Jihad" is not only a supporting or complementary tactic to wage Jihad – for example for propaganda, recruitment, communication, raise funding, preparation of attacks etc., but has become an essential part of the strategy deployed by terrorists – i.e. use digital vulnerabilities to launch attacks and create terror, spy on law enforcers, infiltrate into certain organizations etc.[4]

[1] L. Weinberg, A. Pedahzur & S. Hirisch-Hoefler, 'The challenges of conceptualizing terrorism', Terrorism & political violence, 2004.

[2] D.E.Denning, Cyberterrorism, USA,2000.

[3] Boeke Sergei &Hoogstrate André, cyberterrorisme : veel woorden maar weinig daden, Leiden University,2016.

[4] Jihadisten en het internet, Nationaal coördinator Terrorismebestrijding,2009

An example of the latter would be a digital 9/11 style attack, where the control of airplanes is taken through electronically hacking the flight control systems instead of physically hijacking them. Other targets with electronic vulnerabilities are the

power grid, navigation systems, critical defense systems, self-driving cars, robotic systems, data-critical data-centers, the use of commercial available drones (like used from The Houthi's in Yemen against Saudi) etc. All of them greatly reduce and sometimes even eliminate the need for physical boots on the ground and suicide terrorists.

To prevent such threats requires for our security services to adopt a completely different security approach as in the past. It is no secret that our current society, including military developments, depends increasingly on internet, robotics and electronics with all of them not immune and vulnerable to hacking and cyber-attacks.

Much of online jihad is can be traced back to then Al-Qaeda leader Osama Bin Laden, in his call for jihadists globalization launched back in 1998, under the banner of "the international front of jihad against the Jews and the crusaders", accompanied by cross-border digitization of both ideology, communication and coordination. One of the advantages of cyberspace is that it cheap, efficient and partly anonymous.

Today the goal is not only cyber-terrorism but also to create a global virtual Ummah. To attract Muslims for such a cause, Islamists tend to refer to historical inspirational Muslims. A typical example is the famous world traveler Ibn Battuta (died 1369) who traveled the world for 27 years from Morocco to China and covered a distance of 140 000 km, hailing him as a globalist and role model of how to transcend borders and nations.

RADICAL ISLAM AND CYBER-JIHAD

After the defeat of the caliphate, IS vowed to continue the armed jihad, even against other Muslims[5] through four mechanisms :

- Globalization of Jihad.
- Leveraging on the "breeding grounds" of extremism such as geopolitical conflicts, in particular those where Muslim populations or minorities can be

[5] Deliberate strategy used by IS, by first fighting the close enemy (the corrupt Islam world) as opposed to Al-Qaeda who fight the distant enemy principle (the decadent West) is outlined in Abu Bakr Naji's book " Management of Savagery " or the Application of Cruelty.

victimized, as an instrument for creating sympathy for their cause, create polarization and demonize the "enemy".

- An emphasis on the promotion of the "Virtual Caliphate" and a " Electronic Jihad"
- A specific focus on extending previous successful efforts to ideological empower through hate and mobilize minors under the age of 18 - previous mainly recruited from the major cities in Syria and called the Achbal Al Khilfa (the cubs of the caliphate), and to trigger sleeper cells and lone wolves.

The propaganda, hate speech, perverted ideology used by religious extremists groups with the aim of sawing fear, discord, polarization and hate in society was at least partly successful and as such received, rightfully so, a lot of media attention.

It took till October 2017 for representatives of all major social media players such as Google, Microsoft, Facebook and Twitter, together with the interior ministers of the G7 countries, during a meeting on the Italian island of Ischia, to reach a historic agreement aiming at curbing and blocking jihadist propaganda material. During the meeting the Italian Minister of the Interior, Marco Minniti, proclaimed that "It is the first time that the G7 countries and the representatives of the main Internet players and social networking sites are sitting around the table together".

The spreading of 'digital jihad literature " is another cyber-tactic deployed by jihadists and radical groups. It is well-known that the hallmark of Jihadism is to promote their case by presenting a very fragmented and ideological revisionist interpretation of the Quran and the secondary sources (Hadith and Sunnah). Through the use of half-truths and emotional discourse the y focus on Muslims who have only a basic understanding of Islam and are disenfranchised with life and society. As a result a whole range of Jihad websites and Jihad Magazines are being publicized, with some of the better known being:

- Youth of the caliphate Magazine
- Agency News Haqq
- Inspire Al Qaida (2010-2012)
- Al –Furqan Media Productions (2016)
- Men-10 (Chatblog)
- Al Hayat Media

- El Dabiq (2016)
- Ghulibati Rum
- Halummu AnsarulHaqq

To illustrate the level of effort put in such publication, we can refer to some of the IS propaganda, consisting of videos and messages in 14 foreign languages.

Even though many websites have been taken offline, new sites and publications keep on emerging and extremism and terrorists groups continue an even sophisticated use of technology, internet and social media to keep in touch with their members and sympathizers, especially through the use of encrypted applications and sites including Telegram, Rocket chat, Rayot, Viber, BCM.

An additional level of sophistication are the usage of spyware and sniffing used to get hold of passwords and take over other sites; the use of fake links and web pages; the encryption of articles, messages and photos ; hiding IP addresses and digital identity; and locating servers outside Europe (often in China and Russia).

CONCLUSION

Even when statistics shows that terrorist incidents are on the decline in Europe since 2017, there is an increasing risk that it is morphing from a physical into a digital threat. Already during its specific targeted propaganda campaigns to recruit foreign fighters for Syria and Iraq, IS demonstrated a level of sophistication, competence and craftsmanship, combining Hollywood-style video quality, music and specific messages to solicit strong psychological states and emotions in youngsters.

Since then terrorist organizations have vamped up programs for the recruitment and competency development of computer scientists and engineers, already developing malware such a black shades to spy on enemies in Syria and gain military advantage.

To counter this rising capability and threat to engage into cyber-terrorism and warfare, it is crucial to allocate additional resources. In particular it will be crucial to understand terrorist groups ' cyber-strategy, the techniques they deploy and identify their potential targets early on. It is also important to be constantly reminded of new vulnerabilities and an increasing dependencies on electronics that comes with further digitization, connectedness and the Internet-of-Things (IoT).

About the BIC

The BIC is an independent, non-profit, think-and-do tank based in the capital of Europe that is committed to developing solutions to address the cyclical drivers of insecurity, economic fragility, and conflict the Middle East and North Africa. Our goal is to bring added value to the highest levels of political discourse by bringing systemic issues to the forefront of the conversation.

Author

Brahim Laytouss | Head of AVERA Department

BIC
BRUSSELS
INTERNATIONAL
CENTER

@BICBrussels @bicrhr BIC

www.bic-rhr.com info@bic-rhr.com

Avenue Louise, 89 1050, Brussels, Belgium Tel:+32 027258466