NATIONAL SECURITY

A VIF Publication

Instructions for authors

Wilayat-e-Internet: Islamic State Cyber Caliphate

Anurag Sharma

Sharma, Anurag."Wilayat-e-Internet: Islamic State Cyber Caliphate" National Security, Vivekananda International Foundation Vol.III (3) (2020) pp. 368-391.

https://www.vifindia.org/sites/default/files/national-security-vol-3-issue-3-article-Asharma.pdf

Article

Wilayat-e-Internet: Islamic State Cyber Caliphate

Anurag Sharma

Abstract

The unique characteristics of the Internet—accessibility, borderless flow, vast global audience, have transformed the nature of communication. Individuals, governments, big corporations, industries, educational institutions, as well as terrorist organisations have established their 'virtual' presence on the Internet, also referred to as the cyberspace. The Islamic State (IS), aka Islamic State of Iraq & Syria (ISIS), aka Daesh (Arabic-language acronym of ISIS), has emerged as a fierce but an organised establishment having its own cabinet/councils and media-wings, including the decentralised cyber divisions—"Wilayat-e-Internet". A projection where terrorist organisations could control and coordinate an attack on the interconnected cyber networks is not a fiction. As terrorist organisations, including Islamic State, actively garner the knowledge and skills of deep Internet, it is essential for government institutions and tech industries to upgrade the existing technologies and its effective deployment to counter their growing presence in the Cyberspace and the threat they pose to the global society.

> "The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner".[1]
>
> Ban Ki-moon, Former Secretary-General of the United Nations

According to the data of 2019 report by *International Telecommunications Union,* the usage of the Internet represents 53.6 per cent or 4.1 billion people of the global population[2]. This

Anurag Sharma, Research Associate at Vivekananda International Foundation .

data is a strong evidence of the significant role and impact of the Internet on everybody's life in modern times. Some of the best qualities of the Internet— accessibility, availability, borderless flow, potential to address a vast audience, and speedy transmission of information have revolutionised communications worldwide. It has also enabled terrorist organisations to achieve their objectives. Almost every terrorist organisation or group has established its 'virtual' presence in the cyberspace (also refers to the Internet). The virtual presence of terrorist organisations is not static but dynamic— emergence, modification, and disappearance of the website or content. The term 'cyberspace' and 'the Internet' are not different things but are closely interrelated. Therefore, both terms are used here.

In his book "*Politics on the Nets: Wiring the Political Process"* (1997), Wayne Rash had highlighted eight political uses of the Internet — strategic communication, organisation, recruitment, fund-raising/funding, political positioning, media relations, mobilisation of sympathisers, and international connections.[3] Similarly, terrorist organisations are active in the cyberspace and use the power of the Internet for some or all of the eight purposes highlighted by Wayne Rash. The subject has not been extensively researched in social sciences. There has been also a lack of close attention by policymakers and anti-terrorism agencies to the virtual presence of Islamic State and other terrorist organisations, while widely exaggeration on the threats posed by to 'cyberterrorism'. This paper discusses the various purposes for which terrorist organisations utilise the Internet to achieve their objectives. In later sections, the paper highlights the Islamic State's presence on the Internet, various units of Islamic State's Virtual Caliphate, the "cyber jihadis", and finally, counter-measures and projections.

...the Internet has become the favourite medium of terrorist organisations for their operations, such as recruitment, fund-raising, target profiling...

The Cyberspace: Terrorists' "Not-So-Secret" Playground

With its power of easy accessibility, the speedy transmission of information and anonymity at request, the Internet has become the favourite medium of terrorist organisations for their operations, such as recruitment, fund-raising, target profiling and others. Terrorist activities on the Internet has adopted a dynamic milieu where websites or forums suddenly emerge and disappear. In the past, some shreds of evidence have highlighted that terrorist organisations have been interested in attacking the Critical Infrastructures (CI) of any nation. For example, during the war on terror post-9/11 attacks,

some confidential documents about SCADA (Supervisory Control and Data Acquisition)[1] systems were found in the caves used by al-Qaeda operatives in Afghanistan. As another example, the members of the Irish Republican Army (IRA) had conspired cyber-attacks on crucial supply systems.[4] In today's scenario, an assumption that terrorist groups cannot control the Information Systems and coordinate the attack on the integrated cyber network is misplaced. It is a real-time probability as the groups have already started acquiring and equip themselves with the vast knowledge of the working of the deep Internet.

What are terrorist organisations attempting to gain from their virtual presence? Similar to the statement made by Wayne Rash in his book, in 1999 researchers Steve Furnell and Matthew Warren elaborated the core activities of any terrorist organisations as-- propaganda, fund-raising, dissemination of the information, and secure channels of communications.[5] In his report, *WWW.terror.net: How Modern Terrorism Uses the Internet,* Professor Gabriel Weimann elaborated eight ways in which terrorist organisations are utilising the Internet: psychological warfare, publicity, data mining of possible targets, fund-raising, recruitment of sympathisers and potential terrorists, networking among groups, information sharing, and planning an attack.[6] In modern times, the essential infrastructure sectors of our society, such as banking, healthcare, government, transportation, and to an extent manufacturing capabilities, are mostly dependent on the cyber environment and its structure. A disruption in the services of any of these pillars could result in a catastrophic impact on the nation. Therefore, the probability of a terrorist attack coordinated through the Internet or other Internet-enabled tools cannot be ignored. Based on different studies and the work of Maura Conway's *Terrorists Use of the Internet*[7], the following section determines the four core activities carried out by any terrorist organisation, including the Islamic State (IS), through the Internet.

Publicity/Propaganda

In 1985, then-British Prime Minister Margaret Thatcher addressed the American Bar Association and emphasised in her speech that "[democratic] nations must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend".[8] For any terrorist organisation, publicity or propaganda is the survival kit, be it in the real-world or virtual world. The propaganda of the deed or publicity could be understood as an information of any nature, ideas or special appeals disseminate to 'influence' the opinions, sentiments, attitudes or change in behaviour of a specific or targeted group to benefit the sponsor of the propaganda further, either directly or indirectly.[9] In the virtual

1 Note: SCADA is a computer system for gathering and analysing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

world, the power of the Internet has significantly aided the Islamic State to gain from the opportunities of the publicity of its operations. In the first of its kind, the IS has sophistically utilised the Internet as a tool to spread its propaganda and gain worldwide publicity which attracted many Muslims, including converts to join the world of terror as the foreign terrorist fighters. The time had moved ahead from when the propaganda was disseminated through speeches or blurred videos of the leader of the terrorist groups on certain news media channels, such as al-Jazeera. To gain unmatched publicity against other terrorist organisations on propaganda, Islamic State injected the dynamism in the dissemination of it through videos which tells a story—an exciting story to its viewers, depending on the categories they belong. To meet the purpose effectively, Islamic State used its websites and social media platforms such as Facebook (initially), Twitter, Telegram, and YouTube.

Among the foreign terrorist fighters, many jihadists used to play the role of "jihadists videographers" producing tailored content for the audiences. Generally, the videos were shot in high-resolution featuring documentaries to daily lifestyle in the Caliphate (IS-controlled region of Iraq and Syria) to the execution of its captives. The execution video of the captive US journalist James Foley was one of the propagandist videos by the Islamic State, which attracted significant media coverage worldwide. James Foley was among several journalists, most of them freelancers, who had no backing support from the media organisations and had disappeared during 2012-2013 in Syria. On his execution day on 19 August 2014, the beheading video of James Foley was the title "*A message to America*" floated on *YouTube*; later taken down but re-emerged in other social-media platforms.[10] Scholar Christopher Gunther has analysed James Foley's execution video and says it was part of a propaganda and professional media strategy. Unlike the audio-visual content of Islamic State's predecessor group—al-Qaeda, Foley's execution video had a clear messages of revenge and the reversal of the situation, showing him in 'orange suit' similar to the prisoners of Guantanamo prison.[11] The videos of Islamic State highlight not only the engagements of its fighters in the battlefield with hostile forces, but also project the Caliphate as a well administered State where fighters are praying and reciting verses together, having fun, going for swimming, or a tour of the city organised by other jihadists. The aim of these propaganda videos is not only to boost the fighting strength of the organisation but also to expand it by attracting professionals such as medical practitioners (doctors), academics and educationists who contribute to its image and enabled the Islamic State to be projected as a professionally organised well administered functioning State.

Financing/Fund-Raising

One of the main components of the survival of any terrorist organisation is its

financial health. If publicity is the oxygen, then financing provides the energy to operate an organisation. Money is the lifeline and an engine of an armed struggle.[12] The Internet has provided several options for terrorist organisations to engage in illicit financial transactions, propagate fundamentalism, and radicalisation in either way of *Hawala* networks or through donations received by their illicit association with charity organisations or not-for-profit organisations (NPOs), such as Pakistan-based Lashkar-e-Taiba's Falah-e-Insaniyat Foundation, and Hamas' social service wings.

According to France's renowned anti-terrorism investigator— Jean-Francois Ricard, most of the Islamist terror groups are fulfilling their financial needs through credit card scams. Most of the terror plots in Europe and North America were financed strategically through credit card frauds.[13] The Islamic State has been exploiting the unstable-unpredictable political, security and economic situation of the countries across Middle-East and North Africa region to ensure its financial stability. During the time of Islamic State's predecessor Al-Qaeda in Iraq (AQI) or Islamic State in Iraq (ISI), the organisation was well-financed by the external States and individual wealthy financial sponsors.[14] According to a data, the ISI (Islamic State of Iraq) under the leadership of Abu Musab al-Zarqawi and later, Abu Bakr al-Baghdadi, used to earn USD 70-200 million annually from oil smuggling and USD 36 million as ransom money from kidnappings.[15]

Today, significant evidence has been found to show many terrorist groups have established entities to advance internet-related front businesses to fund their terrorist activities. On 08 November 2019, the Indian Minister of State for Home Affairs (MoSHA)— G K Reddy addressed the conference "*No Money for Terror*" held in Australia, and emphasised that Pakistan-based terrorist group Lashkar-e-Taiba (LeT)'s frontal charity organisation Falah-e-Insaniyat Foundation (FIF) remained very active in the cyberspace despite being banned as a terrorist organisation by the United Nations.[16] The Falah-e-Insaniyat Foundation was founded by the LeT chief and the most-wanted terrorist Hafiz Saeed. As another example, Minister Reddy pointed out the vicious activities of another Not-for-Profit Organisation (NPO) — Islamic Research Foundation (IRF), which was founded by radical Islamic preacher Zakir Naik.[17] The Government of India (GoI) has banned the activities and declared IRF as a proscribed organisation due to its involvement in radicalisation and propagating terrorism.

Networking/Recruitment

The use of the Internet for networking purposes enable the decentralised phenomenon and allow the members of the terrorist organisation to communicate and coordinate effectively. As a small example, the linking capabilities of the Internet enables

the core or central command of the terrorist organisation to link with their affiliate groups and further affiliate groups to link with the main website of the terrorist organisation. Islamic State utilised the power of the Internet to connect with thousands of sympathisers and potential jihadists to join the terror organisation. Several connections were built on social networking platforms for one-to-one communication using 'chat' services available on the Internet, such as ChatSecure, TextSecure, and Redphone.[18]

As IS faced adversaries from the US coalition forces and began to lose territorial control, the virtual Caliphate became more decentralised. The Internet offered the platform to IS's sympathisers at different locations to communicate easily while being 'staying low'. For the networking purposes, Islamic State's cyber team established virtual communities via chat rooms in order to sustain the propaganda, online training (on making bombs or other manuals), and recruitment. Propaganda alone cannot do the magic of radicalisation or recruitment, unless there is a direct engagement from the recruiter, be it offline or online. The recruiter may share the propaganda via the Internet to recruit minors or youth via cartoons or online video games. Islamic State has designed and developed an online game— "Call of Jihad", which is similar to the online game—"Call of Duty".

Considering the recruitment strategy, the IS has carefully designed the cover-page of its online game—Call of Jihad: Operation Assad. Offered in various languages to appeal to a broader audience worldwide, the game— Call of Jihad promoted a sense of adventure to the potential jihadists by offering virtual use of violence against a State or a prominent political identity, rewarding virtual successes.[19] Through the Internet, the Islamic State was able to spread its recruitment and mobilisation of terrorists beyond the local and regional levels, to a worldwide network.

Information Gathering/Data Mining

Today, organisations and individuals publish a large amount of information about their activities and insights of the businesses. Terrorist organisations may use available search engines or Dark Net technologies to obtain information about their specific target. Easily available and publicly accessible information such as real-time closed-circuit television (CCTV) footages, and detailed longitude and latitudes from Google Earth application can be used by terrorist organisations to get high-resolution satellite images or specific information about terrain for reconnaissance or recce of the target. Islamic State has been utilising the Internet to gather information on targets for terrorist operations, and of individuals to advance radicalisation or recruitment purposes. *Facebook*, *Instagram*, *Twitter* and sometimes *Snapchat* profiles are scanned to see if an individual is an IS (Islamic State) sympathiser and may qualify as a recruit. Recruiters add these sympathisers as 'Friend' and

engage in private communication with them after a while.

Unsurprisingly, apart from the officials of intelligence fraternity- not many people may have heard the name of Zarrar Shah— a Pakistani national and technology chief of Lashkar-e-Taiba (LeT). In the 2008 Mumbai attacks, Zarrar and other conspirators of the Mumbai attack used Google Earth satellite imagery services to guide terrorists through the routes to their respective targets in Mumbai (Bombay) city. To disguise his location, he established an Internet phone system and routed his communication through New Jersey, US. However, since September 2008, the British intelligence agencies were tracking Zarrar's online activities and messages; but they failed to put the picture together of the conspiracy of the attack for their Indian intelligence counterparts.[20]

Islamic State's Cyber Caliphate

In mid-2014, Islamic State (IS)'s self-claimed Caliph and its leader Abu Bakr al-Baghdadi rose to the stairs of the podium of a Mosque in Mosul, Iraq and made a call to Muslims worldwide to do *Hijra* (Arabic term for emigration) to the newly formed Caliphate State in Iraq and Syria. As a terrorist organisation, the IS had emerged from being an old franchise of a popular terrorist group— Al-Qaeda in Iraq (AQI), later known as the Islamic State in Iraq (ISI). The call made by al-Baghdadi had an unbelievable outcome for the expansion of IS's contingent. The mobilisation of Muslims worldwide to join jihad and fight alongside IS as foreign terrorist fighters (FTFs) surpassed the number of jihadists in the 'mother of all jihads'— the war against the Soviet forces in Afghanistan during 1980-1992. Was it the charisma of al-Baghdadi's voice solely responsible for convincing the foreign terrorist fighters and supporters to travel to the IS-controlled territories in Iraq and Syria? In fact, an equally important role was played by the Internet in building up and sustaining the virtual image of the IS's Caliphate. As per the Islamic State's ideological project, the terrorist organisation was using the Internet as one of the vital weapons in its arsenal. Through the Internet, the IS had managed to intimidate its opponents and promote itself by transmitting texts, photos, handbooks/manuals, and its famous *Dabiq* online magazine, which featured everyday life of a foreign terrorist fighter and brief reporting of the events. In the history of terrorism, no terrorist organisation has understood and utilised the power of the Internet as much as the IS did and still does. Strategically and in a sophisticated manner, the IS has created a web of social media accounts which show that the sympathisers of the terrorist organisation are everywhere, despite the organisation's downfall and territorial loss, followed by the killing of its popular Caliph— Abu Bakr al-Baghdadi.

Among its virtual presence on various social media platforms, such as *Facebook*, *Vkontakte* (VK), *Telegram* and others, *Twitter* was the most significant network for IS. One

of IS's most successful projects was an Arabic-language *Twitter* application (app), 'The Dawn of Glad Tidings' or 'Dawn'.[21] The Dawn of Glad Tidings was projected as a medium to stay up to date with the news and events about the organisation. Upon successful download and sign-up, the application syncs with the user's Twitter account and posts tweets or messages, such as hashtags (#), images, and other links, to the user's account. The same content can be tweeted and re-tweeted by anyone who signed up for this application. During this, the twitter account of the user would work as it used to be.

But, with the sophisticated synchronisation of the *Twitter* account and the application, the IS's social-media operation team technically managed to avoid triggering the *Twitter*'s spam detection algorithm.[22] The Dawn of Glad Tidings app survived merely for two months, i.e. April-June 2014; however, the existence of the app had come into the limelight of the counter-terrorism circle after the Islamic State exploded in the news of its capture of Mosul.[23] The Dawn of the Glad Tidings app had generated up to 40,000 tweets in a day, but the termination of this app on 17 June gave a blow to the propaganda strategy of the Islamic State.[24]

After two events in 2015— i) the revelations made by US NSA (National Security Agency) contractor—Edward Snowden on the US snooping and privacy invasion, and ii) and, the taking down of hundreds of Islamic State websites on cyber domains post-2015 November Paris attacks, many Islamic State sympathisers migrated from open Internet to the Dark Web. The Dark Web or Dark Net refers to the platform where the content exists in encrypted form and is not indexed by the conventional search engines. In the case of terrorist organisations, Dark Web is a favourite platform for propaganda, fund-raising, procurement of illegal weapons, facilitating illegal transactions using crypto-currencies such as Bitcoin.[25] In view of the migration, Al-Hayat media centre—a regular media outlet for Islamic State-- posted guidelines on Telegram channel about accessing the Dark Web.

Three significant units— Al-Hayat Media Centre, Amaq News Agency, and United Cyber Caliphate of the Islamic State -- were extensively involved in the dissemination of propaganda and carrying out cyber-related operations of the terror organisation. Since the time of Islamic State's self-declared Caliphate in 2014, Al-Hayat Media centre has been its most important media wing, which targets the audience from the West and disseminates the relevant content in English, German, Russian, and French.[26] By June 2017, IS was in retreat having lost of over 60 per cent of territories captured during its peak time (2014-2016). Despite the loss of physical territories, the IS was conquering and dominating the cyberspace through its social media and cyber Caliphate. Yet, most powerful militaries failed to digest the fact that a dangerous influence can be easily transmitted through either

a one-touch (on smartphones) or a click (on computer systems). Policymakers and counter-terrorism analysts too overlook the Islamic State's cyber capabilities and the use of the Internet to lure the sympathisers worldwide.

Al-Hayat Media Centre

The propaganda videos were produced by Islamic State's media wing—Al-Hayat Media Centre (AMC). Established soon after the declaration of Islamic State's Caliphate in mid-2014, AMC carried out the responsibility of disseminating the information, speeches, and other communication for the terror organisation. The logo of Al-Hayat Media Centre is very similar to the logo of popular Middle-East based news network— Al-Jazeera. In July 2014, al-Hayat began the publication of its popular digital magazine *Dabiq* which was later published in many languages, including English. Primarily, Dabiq focused on the radicalisation and recruitment of the people and lured them to join the Islamic State. The name of the magazine was an inspiration from a town 'Dabiq' in Northern Syria which has significance in the *hadiths* regarding the Armageddon.[27]

The magazine Dabiq, mainly the first issue, intended to capture the attention of the Muslims around the world, especially youth, and inspire them to join the IS. The presentation of the magazine and emigration of worldwide Muslim to join jihad alongside IS was a clear indication that it's Caliph 'al-Baghdadi' had some serious plans. Along with Dabiq, AMC also produced other magazines which built a significant presence in the virtual world. Al-Hayat had also started publication of two other digital magazines, in the Turkish language. The first was *Konstantiniyye* (the Ottoman word for Istanbul), which discussed IS's strategic and political approach as well as international events, and provided its perspective on Turkish politics.[28]

However, *Konstantiniyye* was discontinued for unspecified reasons and was replaced by another digital magazine— *Rumaiyah*—the Arabic word for Rome. It was the AMC that released a propaganda video featuring British war journalist—John Cantlie, taking a tour of the city of Aleppo and taking interviews of the locals.[29] The strategy behind the video was to highlight the ruins of the city caused by *Kufars* or hostile forces, and John Cantlie as a face representing western media. In 2012, John Cantlie was kidnapped in Syria. By the year 2017, AMC had its Telegram (application) channel/group where videos, images, and documents related to the propaganda and activities of the IS were uploaded. Several jihadis and sympathisers were part of these channels.

On 31 December 2017, the AMC released 'Nasheed' (a work based on vocal music): "O Disbelievers of the world" targeting the US President Donald Trump, Syrian President

Bashar al-Assad, Russian President Vladimir Putin, Israel's Prime Minister Benjamin Netanyahu, and French President Emmanuel Macron.[30] The video was a clear warning to the world leaders over their alliance against the Islamic State. Due to the clean-up process targeting jihadi and extremist content online undertaken by social media platforms in 2015-2016, mainly Twitter, Islamic State's AMC moved its propaganda to a more confidential and secure platform—Telegram. Considering AMC as one of the core parts of the Islamic State, the US Department of State on 21 March 2019, designated AMC, Amaq News Agency and other IS related groups Foreign Terrorist Organisations (FTO) under Section 219 of the Immigration and Nationality Act, and also as a Specially Designated Global Terrorist (SDGT) under the US Executive Order 13224.[31]

Amaq News Agency

Amaq News Agency (ANA) is the Islamic State's news outlet. The main purpose of ANA is to disseminate the claim of an attack worldwide. In 2013, Rayan Machaal *aka* Baraa Kadek—a Syria-based journalist and seven other members of Halab News Network, who later joined the IS, had founded ANA.[32] It came to the limelight with the reporting of the Siege of Kobani (Syria) in 2014. Soon, the ANA became a known identity among western media after it began reporting the claims and responsibilities of terrorist attacks, including the 2015 San Bernardino attack, and the 2019 Sri Lanka Easter Bombings, among others. Progressing towards more sophisticated tools of the Internet, in 2015, ANA designed and launched its official application (hereafter app) and issued a warning against unofficial versions available on the Internet which may spy on the registered users—Islamic State operatives and sympathisers worldwide. The idea behind the official app was to broadcast real-time operations from the battlefield to Islamic State supporters over the Internet.[33]

Apart from the official app, ANA maintained a Word Press portal which contained high-resolution images along with news headlines. However, in a sudden move, the Word Press account was taken down in April 2016.[34] A new generation of tech-savvy jihadists has emerged in the era of freely available and easy to use encrypted and secure messaging apps such as Telegram and WhatsApp. ANA also had several channels on Telegram app, which appeared and disappeared from time to time. Among other groups/channels of Islamic State on Telegram, a channel— "Did You Know?" existed which attempted to depict Muslims as superiors in comparison to the westerners and criticised cultures other than Islamic. Targeting Hinduism as a religion and culture of India, the channel—"Did you know" stated that practice of Yoga is similar to being in association and interacting with the devil.[35]

Considering the similar nature and operations of ANA and the other Islamic State media outlet AMC, the US Department of State on 21 March 2019, designated ANA and

all its manifestations as Foreign Terrorist Organisation (FTO) under Section 219 of the Immigration and Nationality Act, also as a Specially Designated Global Terrorist (SDGT) under the US Executive Order 13224.[36]

United Cyber Caliphate

During its rise in 2016 the Islamic State also established the United Cyber Caliphate (UCC) or Islamic State Hacking Division (ISHD). The UCC was a decentralised group consisting of several 'high-tech' clusters of Crackers[2] who further identified themselves as the digital army with allegiance to the IS worldwide. UCC was built with an army of sophisticated Crackers working on their computer systems, and intimidating their distant enemies just as a terrorist does to the people on the ground. Junaid Hussain— a British-Pakistani Cracker was one of the primary members of the UCC, who gave new dimensions to cyber operations of the Islamic State. The UCC had four sub-groups: Cyber Caliphate Army (CAA), Ghost Caliphate Section (GSC), Sons of the Caliphate Arms (SCA), and Kalashnikov e-Security. Decentralised in nature, the main activities of the UCC and its sub-groups were carrying-out cyber operations, recruiting new sympathisers, and offering cyber-security guidelines and awareness on how to stay low, undetected and carry out terrorist attacks.[37]

Since its birth in mid-2014, IS's UCC has carried out eight successful cyber-attacks, which highlights the sophisticated cyber capabilities of this group and its cyber jihadis. The year 2015 was the most successful year for the

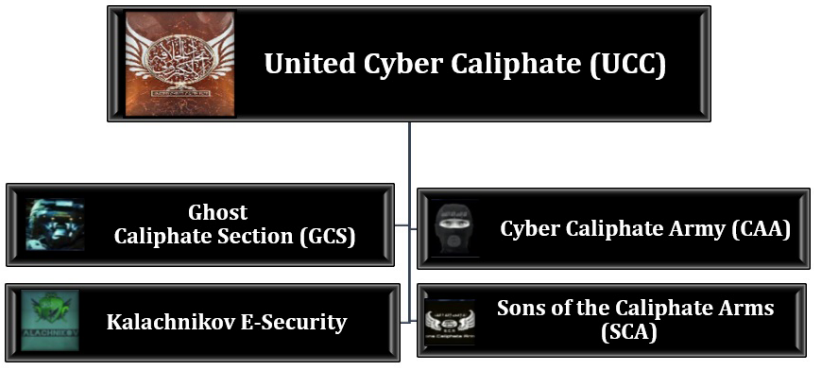
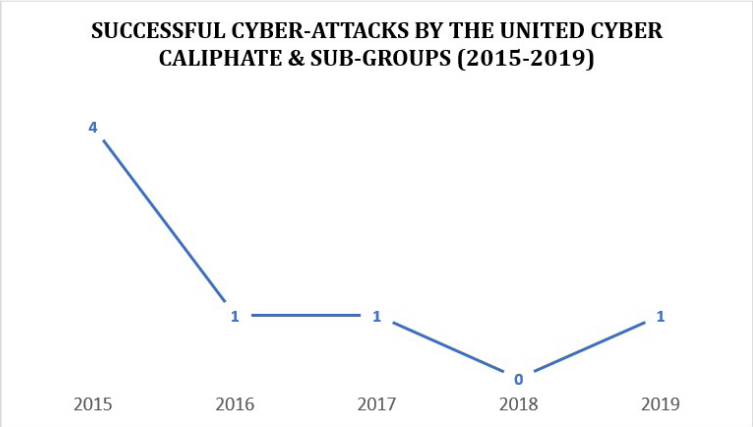


Chart 1: Sub-groups of Islamic State's United Cyber Caliphate [Info. Source: Twitter/MEMRI]

In 2015, the cyber jihadis of the group carried-out four cyber-attacks in five months. It started with a successful attack on 08-09 April 2015, when the UCC attackers targeted the French Television Network TV5Monde and hijacked its websites and all social media

2 Note: The author deliberately uses the word Cracker and not the 'Hacker'. Understanding the fact, there is a difference between a hacker and a cracker. A Hacker constantly seeks knowledge and freely share their discoveries and never damage data intentionally. However, a Cracker is all opposite of a Hacker; breaks into the system with malicious intent.

networks. The TV5Monde has been targeted because of its outreach and audience in 200 countries. Targeting the TV5Monde's Facebook page, the UCC attackers posted the ID cards and CVs of the relatives of the French soldiers involved in US-led coalition forces against the IS in Iraq and Syria.



Graph 1: Number of successful cyber-attacks carried out by the United Cyber Caliphate (2015-2019)

The crackers also posted a warning message to the French troops that "*they [French soldiers] must stay away from the Islamic State. It is an opportunity for them to save their families, and they shall take advantage of it. The cyber-caliphate shall continue its cyber-jihad against the enemies of Islamic State*".[38] However, Cyber-security experts had a different opinion on the attack. According to the US-based security firm *FireEye*, there are similarities in the pattern of attack on TV5Monde network and the pattern used by the Russian crackers of a group known as AT28.[39] Given the offensive cyber-skills of the UCC, it was highly likely that the attackers had utilised the compromised IP (Internet Protocol) addresses of the AT28 for coordinating the cyber-attack on French TV5Monde network.

On 13th April 2015, the UCC attackers had targeted and taken down the website and host servers of Australia's Hobart International Airport in Tasmania and placed banners of Islamic State and supporting statements on the main page of the website.[40] This was followed by two successful cyber-attacks in April. The UCC carried out significant attacks in August and September 2015 targeting two long-lasting allies in the war against Islamic State— the United States and the United Kingdom, respectively. On 12 August 2015, the UCC attackers published an MS-Excel spreadsheet containing the names, e-mail addresses, phone numbers, and passwords of 1400 members of various US military and government institutions, including the United States Marine Corps (USMC), the NASA, the US Department of State, the US Air Force, and the Federal Bureau of Investigation (FBI).[41]

The message posted along with the list urged the supporters of the IS to act as lone wolves and kill the people mentioned on the list. The cyber-attack was led by Junaid Hussain who had been a critical profile in the UCC and was enlisted at number three on the CIA's "kill list" of the IS operatives and supporters. Junaid Hussain was killed on 24 August 2015 in a US drone strike.

On 11 September 2015, the cyber jihadis targeted and intercepted 'top secret' e-mail communications of the British Government. The investigation carried out by the Government Communications Headquarters (GCHQ) revealed that Islamic State's cyber army had been targeting the information related to then-Prime Minister David Cameron, then-Home Secretary Theresa May, and the list of events that senior government figures and members of the Royal Family were likely to attend in following months.[42] On 15 April 2016, in another successful cyber-attack, the UCC cyber jihadis attacked 20 small businesses in Australia and defaced their websites with the following message: "*In the name of Allah, we are United Cyber Caliphate. Obey the Islamic State. Your [Australia] system is failed. Islamic State #rules*".[43] In April 2017, the UCC made another comeback with an attack on US servers and released the "kill list" with the message to "kill them wherever you find them", giving instructions to would-be attackers to kill 8,786 people, including the US President Donald Trump.[44] The most recent cyber-attack claimed by the UCC was in July 2019 in which one of the sub-groups of the UCC claimed to have hacked 150 Twitter accounts of random people.[45]

Islamic State's Cyber Jihadis

With its rise and successful terrorist operations in Iraq and Syria, the Islamic State has been recruiting the Crackers for joining the divisions of its Cyber Caliphate. According to J M Berger—a researcher on extremism and the co-author of *ISIS: The State of Terror,* some recruits joined Islamic State as a collaborator at a distance, while others emigrated to Syria. As part of their roles, these cyber jihadis are responsible for targeting western nations on cyberspace, maintaining Internet access in IS-controlled territories, and guiding other operatives on related security issues.[46] Below are some of the well-known cyber jihadis who contributed to the growth of the virtual Caliphate of Islamic State with their tech-savvy skills.

British-Pakistani Face of Cyber-Savvy Jihadism: Junaid Hussain

Junaid Hussain was a British-Pakistan Cracker and a propagandist for Islamic State under the pseudonym Abu Hussain al-Britani. In 2012, Junaid Hussain was arrested and jailed for cracking into then-British Prime Minister Tony Blair's account and publishing his personal information over the Internet. He had also blocked the police's anti-terrorism

hotline.[47] As a mistake in Junaid's prosecution, the defence lawyer in the Crown Court considered the online exploits as a childish prank. Within a year, Junaid Hussain travelled to Syria and emerged as one of the most dangerous cyber jihadis for Islamic State. Being a key member of Islamic State's Cyber Caliphate, Junaid Hussain was the main suspect in a coordinated cyber-attack on 12 January 2015 on the *Twitter* and *YouTube* accounts of the US Central Command or CENTCOM.[48]

Junaid Hussain was a lethal weapon in the Islamic State's virtual arsenal. Junaid's cyber jihadism was so threatening to the western nations that the United States listed him as the third-highest IS target on the Pentagon's "Kill List" after the then-IS leader Abu Bakr al-Baghdadi (later killed in October 2019) and Mohammad Emwazi *aka* Jihadi John (November 2015).[49] In the history of War on Terror, Junaid Hussain, at the age of 21, became the first Cyber Jihadi or Cracker to be killed by a drone strike on 24 August 2015. He was married to IS's jihadi bride—Sally Jones *aka* Umm Hussain al-Britani, who denied the killing of her husband Junaid via tweets on two Twitter accounts linked to the IS. [50]

A Curious Case of an Indian Cyber Jihadi

On 13 December 2014, Indian security agencies arrested one of the most followed and significant 'virtual' sympathisers of Islamic State.[51] Mehdi Masroor Biswas— a 24-years-old (as of 2014) electrical engineer by profession, Mehdi was working as an executive in a multinational company based in Bangalore, Karnataka. At the time of his arrest, Mehdi was the administrator of the most influential pro-IS Twitter handle/account—@ShamiWitness. During the peak time of the IS, from mid-2014 to 2015, @ShamiWitness had over 17,000 followers, and a viewership of two million times each month of his tweets. @ShamiWitness emerged as the most influential pro-Islamic State Twitter handle on the Internet.[52]

According to the report by *The Times of India,* Mehdi had assumed that the Indian security agencies might never catch him as he used a pseudonym over the Internet.[53] While communicating with other potential jihadists or pro-IS sympathisers over the Internet, Mehdi introduced himself as a Libyan citizen living in the United Kingdom (UK) and had never revealed his real identity or location to anyone. In an interview with UK's *Channel 4 News*, Mehdi Biswas admitted that he was impressed and sympathised with the ideology of the IS. "If I had the chance to leave everything and join them (IS) I might have….but my family needs me here." Mehdi had expressed his willingness to work for the terror group [Islamic State].[54]

Another Case of Cyber Jihadi: Muddabir Mushtaq Sheikh

During mid-2014 and 2016, social media in India had been a hunting ground for Islamic State recruitment. Another Indian cyber jihadi for Islamic State had emerged from Maharashtra. In February 2016, NIA had arrested 14 people in connection with their links with the Islamic State. Among the 14 arrested, Mudabbir Mushtaq Sheikh *aka* Abu Musab— a 34 years-old Software Engineer from Mumbai, Maharashtra, was involved in the recruitment of youth from India for Islamic State over the Internet.[55] Mudabbir's *modus operandi* to recruit online had included the random search for social media accounts of people who reacted 'positively' on the propaganda of Islam and had watched videos of radical speeches by various Islamic clerics.[56] After this, potential individuals were traced, contacted and then encouraged to join the Islamic State.

During his interrogation, Mudabbir had revealed that before the 9/11 attacks in 2001, he had completed his Higher Secondary education and had married. He was disturbed by the accusations that emerged post-attack on the Muslim community, labelling them as terrorists. In 2003, Mudabbir completed his graduation and web-designing course simultaneously, and thereafter till 2012, he worked as a web designer in various establishments. After losing his job with *Sportz Interactive* in Mumbai, Maharashtra in 2014, Mudabbir used to spend time on the Internet, reading about the emergence of the Islamic State. During a curious probe on the Caliphate over the Internet search engine, Mudabbir came in contact and became friends with Yousuf al-Hindi *aka* Shafi Armar on *Facebook*. Shafi Armar was none other than the former member of Indian Mujahideen (IM) under the leadership of Riyaz Bhatkal.[57] Mudabbir became the self-declared chief of Junood-e-Khalifah al-Hind (JKH)—an Islamic State-inspired radical group in India. The investigation in the Mudabbir's case also revealed that he used to communicate with other jihadists of the group (JKH) through 'Trillian' and 'Surespot' messenger applications.[58] These applications had an additional layer of encryption which makes it tough for security agencies to track the communications.

Countering the Virtual Caliphate

Internet is one of the essential elements for any terrorist organisation to "stay alive" in the current era. The Internet facilitates the rapid and wide sharing of information or exchange of ideology or dissemination of sentiments in the form of propaganda. The dissemination of terrorist propaganda or ideology on social media platforms, however, also trigger a war of words from anti-terrorism groups. The counter-narratives to the propaganda based on factual information may be conveyed through videos and images.

Law-Enforcement

Internet is a 'double-edged' sword for a terrorist organisation. The advancements in the Internet have posed severe challenges for law-enforcement agencies and opportunities for the terrorist organisations to disseminate their propaganda and carry out their activities. However, if the Internet facilitates their propaganda, recruitment, financing, and other activities; then the Internet also registers digital footprints of terrorist organisations with which law-enforcement/security agencies can trail them. Since 9/11 attacks, the law-enforcement agencies have taken many initiatives to disrupt the advancements of terrorist organisations worldwide. Private organisations and individuals too have joined the agencies in this effort.

The information disseminated on terrorist websites which are hosted on open source domain may also work as a 'warning' system for an attack. For example, two days before the infamous 11 September 2001 attack, a message was displayed on a Dubai-based discussion forum— alsaha.com – which claimed that in the "next two days, a big surprise will be coming from Saudi Arabian region of Asir".[59] Asir is a remote location in Saudi Arabia adjacent to Yemen from where nineteen hijackers of 9/11 attack hailed. At a global stage, law-enforcement agencies/intelligence agencies, including those of India, have been working in cooperation with various technology companies and social media companies such as *Facebook*, *Twitter* and *WhatsApp* (owned by *Facebook*) to understand the role of the Internet and develop the narratives for counter extremism.

The Indian law-enforcement agencies have been working with communities and religious leaders as well. The moment any family identifies a behavioural change in the radicalised youth, the security agencies intervene and stop the mobilisation of the radicalised individual before any act of terror can be committed. The arrests of several IS sympathisers from Southern India is one of the best examples of law-enforcement agencies successfully cooperating with community members in a fight against terrorism.

Private Stakeholders

While the responsibility of countering terrorism primarily lies with the law-enforcement agencies of the nations, the private stakeholders, especially the Internet Service Providers (ISPs) and social media platform companies, have an equal responsibility in countering the terrorist use of the Internet. One of the main approaches from tech companies is to limit the dissemination of extremist content by deploying access controls on the network or by censoring the Internet content, or a combination of both.[60] According to statistics released by the video-content sharing website—*YouTube*, over 2 billion 'logged-

in' users visit it every month to watch over a billion hours of videos and generate billions of views.[61] *Google*, the parent company of *YouTube*, has a policy to swiftly react to reports submitted regarding illicit content and remove the link within six hours of receiving the request, if the request is legitimate.[62]

Another approach to counter the terrorist use of the Internet for radicalisation and propaganda purposes, has been pioneered by the United States-based organisation—*Parallel Networks,* which believes in 'reverse engineering' of the radicalisation process to counter extremism. *Parallel Networks* was founded by Jesse Morton, formerly known as Younus Abdullah Mohammad, a converted Muslim, who was the creator of al-Qaeda's digital magazine '*Inspire*' and its chief recruiter in the West. Under Morton's guidance to counter extremism, *Parallel Networks* introduced a magazine— *Ahul-Taqwa*, which means in Arabic, People of Consciousness.[63] Strategic counter-narrative initiatives such as *Parallel Networks* use the Internet, in different languages, for a worldwide audience. The counter-narratives address the underlying issues which contribute to the online/offline radicalisation.

What Lies Ahead?

The Terrorist use of the Internet is a transnational issue, unrestricted by borders. Therefore, countering the terrorist use of the Internet has to be a collaborative effort of all the countries. Social media platforms, including *Facebook*, *Twitter*, *YouTube*, have in the past allowed terrorist organisations, including Islamic State, to spread their propaganda across the borders in real-time, with sophisticated and high-resolution content. Social media has been a crucial for the mobilisation of Indian youth to join Islamic State as foreign terrorist fighters. Most of these Indians were radicalised by Islamic State ideology online.[64] Unlike al-Qaeda, the Islamic State focused on disseminating the propaganda in regional languages such as Malayalam and Tamil.[65] This was certainly a reason why the mobilisation was more from Southern India. The online release of weekly newsletters—*al-Naba* and claim of attacks by ANA underlines that the territorial loss of Iraq and Syria has not made much of an adverse impact on the cyber operations of the Islamic State. However, since its last cyber operation in 2019, the Islamic State's United Cyber Caliphate has not carried out any operation. Internet surveillance and collection of information on suspects have helped in countering terrorist use of the Internet. However, surveillance of the Internet give raise to questions regarding individual's Right to Privacy, including the identity of the suspect and information on his

Social media platforms, including Facebook, Twitter, YouTube, have in the past allowed terrorist organisations, including Islamic State, to spread their propaganda across the borders in real-time

or her private life. Social media platforms such as *Twitter* and *Facebook,* however, have recently included provisions in their terms and policies that prohibit content that promote extremism or the cause of terrorist organisations. For instance, according to the terms of Twitter— "a user cannot affiliate with and promote the illicit or illegal activities of a terrorist organisation or violent extremist group".[66]

Given that terrorist organisations have always been a step ahead of the security agencies, the allocation of funds for intelligence fraternity of a country should not only utilised over the HUMINT (Human Intelligence) but equally, if not more, utilised for the deployment of enhanced technical capabilities. There will always be a need to constantly upgrade the existing technologies and its deployment in the fight against terrorism. Containing the threat of cyber-attacks by tech-savvy terrorists is vital for defending our societies and the Critical Infrastructure (CI) and adequate funds must be found for it.

References

1. "The Use of the Internet for Terrorist Purposes', United Nations Office on Drugs and Crime." 2012. UNODC. United Nations . September 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
2. "Number of Internet Users", International Telecommunication Union, 2019, Available from: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Stat_page_all_charts_2019.xls
3. Rash, Wayne. 1997. Poltics on the Nets: Wiring the Political Process. New York
4. Blau, John. 2004. "The Battle against Cyberterror." Network World. November 29, 2004. https://www.networkworld.com/article/2327822/the-battle-against-cyberterror.html.
5. Furnell, S.M., and M.J. Warren. 1999. "Computer Hacking and Cyber Terrorism: the Real Threats in the New Millennium?" Computers & Security 18 (1): 28–34. https://doi.org/10.1016/s0167-4048(99)80006-6.
6. Weimann, Gabriel. 2004. "Www.terror.net How Modern Terrorism Uses the Internet." United States Institute Of Peace. March 2004. https://www.usip.org/sites/default/files/sr116.pdf.
7. Conway , Maura. 2005. "Terrorist 'Use' of The Internet and Fighting Back ." Oxford University. September 2005. https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf.
8. Thatcher, Margaret. "Speech to American Bar Association", Margaret Thatcher Foundation, 15 July 1985, Available from: https://www.margaretthatcher.org/document/106096

9. United States. Department of Defense Dictionary of Military and Associated Terms- Joint Publication 1-02, Department of Defense, 12 April 2001, Available from: https://www.cia.gov/library/abbottabad-compound/B9/B9875E9C2553D81D1D6E0523563F8D72_DoD_Dictionary_of_Military_Terms.pdf

10. Bender, Stuart M.. "Not really Hollywood: the media's misleading framing of Islamic State videos", The Conversation, 17 October 2016, Available from: https://theconversation.com/not-really-hollywood-the-medias-misleading-framing-of-islamic-state-videos-66131

11. Stute, Dennis. "Gunther: 'the Islamic State is highly rational'", Deutsche Welle, 20 August 2014, Available from: https://www.dw.com/de/g%C3%BCnther-der-islamische-staat-agiert-hochgradig-rational/a-17866907 [translated from German to English using Google Translator].

12. Napoeloeni, Loretta. "The economy of terror", Open Democracy, 26 January 2005, Available from: http://www.mafhoum.com/press7/225E61.htm

13. Thomas, Timothy L.. "Al-Qaeda and the Internet: The Danger of Cyberplanning", Parameters, Spring 2003, Available from: http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf

14. "Funding ISIS", The Washington Institute for Near East Policy, Available from: https://www.washingtoninstitute.org/uploads/Documents/infographics/Islamic-State-of-Iraq-and-al-Sham-ISIS-Funding.pdf

15. Liang, Christina Schori. "The Criminal-Jihadist: Insights into modern terrorist financing", Geneva Centre for Security Policy, Strategic Security Analysis No. 10, August 2016, Available from: https://dam.gcsp.ch/files/2y10TflBzyeiQACfYZl2yYpaGuBhSe3KV8jrjljD8vV3iRFQyrikhop2

16. PTI. "Hafiz Saeed's terror group active in cyber world: Union Minister", NDTV, 09 November 2019, Available from: https://www.ndtv.com/india-news/hafiz-saeeds-terror-group-falah-e-insaniyat-foundation-active-in-cyber-world-union-minister-g-kishan-2129666

17. Ibid.

18. "ISIS follower on Twitter warns against using Kik messenger service 'when chatting about jihadi stuff', recommend other technologies", MEMRI, 05 November 2014, Available from: https://www.memri.org/cjlab/isis-follower-on-twitter-warns-against-using-kik-messenger-service-when-chatting-about-sensitive-jihadi-stuff-recommends-other-technologies

19. United Nations. "The Use of the Internet for Terrorist Purposes", United Nations Office on Drugs and Crime, September 2012, Available from: https://www.unodc.org/documents/

frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

20. Glanz, James ,Sebastian Rotella, and David E Sanger. "In 2008 Mumbai Attacks, piles of spy data, but an uncompleted puzzle", The New York Times, 21 December 2014, Available from: https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html

21. Berger J.M. "How ISIS Games Twitter", The Atlantic, 16 June 2014, Available from: https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

22. Ibid.

23. Stern, Jessica and J M Berger. 2015. ISIS: The State of Terror. London: William Collins. pg 150.

24. Berger, J.M. "How ISIS Games Twitter", The Atlantic, 16 June 2014, Available from: https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

25. Liang, Chrisrina Schori. "Unveiling the United Cyber Caliphate and the birth of the e-Terrorist", Georgetown Journal, Fall 2017 (Vol 18 No. 3), Available from: https://dam.gcsp.ch/files/2y10J90JJDcWfuIrVEExJU5SuOkDgq8V08daYodqmvT26flfqCIibJmC

26. "ISIS declares Islamic Caliphate, appoints Abu Bakr al-Baghdadi as 'Caliph', declares all Muslims must pledge allegiance to him", MEMRI, 01 July 2014, Available from: https://www.memri.org/reports/isis-declares-islamic-caliphate-appoints-abu-bakr-al-baghdadi-caliph-declares-all-muslims

27. Ryan, Michael W S. "Dabiq: what Islamic State's new magazine tell us about their strategic direction, recruitment patterns, and Guerrilla doctrine", The Jamestown Foundation, 01 August 2014, Available from: https://jamestown.org/program/hot-issue-dabiq-what-islamic-states-new-magazine-tells-us-about-their-strategic-direction-recruitment-patterns-and-guerrilla-doctrine/

28. Akkoc,Razziye and Louisa Loveluck. "Ankara bombings: Islamic State is main suspect, says Turkish PM Ahmet Davutoglu", The Telegraph, 12 October 2015, Available from: https://www.telegraph.co.uk/news/worldnews/islamic-state/11926022/Ankara-bombings-Islamic-State-is-main-suspect-says-Turkish-PM-Ahmet-Davutoglu.html

29. Hayden, Sally. "British hostage John Cantlie 'reports' from Aleppo in latest Islamic State propaganda video", VICE, 10 February 2015, Available from: https://www.vice.com/en_us/article/kz5dj9/british-hostage-john-cantlie-reports-from-aleppo-in-latest-islamic-state-propaganda-video

30. Terrorism Research & Analysis Consortium (@TRACterrorism). 2018. "TRAC's twitter post". Twitter, 08 January 2018, 02:30 AM (IST), Available from: https://twitter.com/tracterrorism/status/950109896426606603?lang=en

31. United States. "Amendments to the Terrorist Designations of the Islamic State of Iraq and Syria", US Department of State, 21 March 2019, Available from: https://www.state.gov/amendments-to-the-terrorist-designations-of-the-islamic-state-of-iraq-and-syria/

32. LeMonde. "Founder of Aamaq, the IS propaganda agency killed in Syria", Le Monde, 31 May 2017, Available from: https://www.lemonde.fr/syrie/article/2017/05/31/un-fondateur-d-aamaq-l-agence-de-propagande-de-l-ei-tue-en-syrie_5136836_1618247.html

33. Russon,,Mary-Ann. "Islamic State: Fake version of ISIS Amaq news app is spying on its supporters", International Business Times, 02 June 2016, Available from: https://www.ibtimes.co.uk/islamic-state-fake-version-isis-news-app-amaq-android-spying-its-supporters-1563313

34. Ibid.

35. Russon, Mary-Ann and Jason Murdock. "Welcome to the bizarre and frightening world of Islamic State channels on Telegram", International Business Times, 02 June 2016, Available from:https://www.ibtimes.co.uk/welcome-bizarre-frightening-world-islamic-state-channels-telegram-1561186

36. United States. "Amendments to the Terrorist Designations of the Islamic State of Iraq and Syria", US Department of State, 21 March 2019, Available from: https://www.state.gov/amendments-to-the-terrorist-designations-of-the-islamic-state-of-iraq-and-syria/

37. Liang, Christina Schori. "Unveiling the United Cyber Caliphate and the birth of the e-Terrorist", Georgetown Journal, Fall 2017 (Vol 18 No. 3), Available from: https://dam.gcsp.ch/files/2y10J90JJDcWfuIrVEExJU5SuOkDgq8V08daYodqmvT26flfqCIibJmC

38. France24. "France's TV5Monde targeted in 'IS group cyberattack'", France24, 09 April 2015, Available from: https://www.france24.com/en/20150409-france-tv5monde-is-group-hacking

39. Sheera Frenkel. "Experts say Russians may have posed as ISIS to hack French TV channel", BuzzFeed News, 09 June 2015, Available from: https://www.buzzfeednews.com/article/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t

40. AFP. "Australian airport website hacked by Islamic State", The Telegraph, 13 April 2015, Available from: https://www.telegraph.co.uk/news/worldnews/islamic-state/11531794/Australian-airport-website-hacked-by-Islamic-State.html

41. Safi, Michael. "ISIS 'hacking division' releases details of 1,400 Americans and urge attacks", The Guardian, 13 August 2015, Available from: https://www.theguardian.com/world/2015/aug/13/isis-hacking-division-releases-details-of-1400-americans-and-urges-attacks

42. Perry, Keith. "ISIS hackers intercept top secret British government emails in major security breach uncovered by the GCHQ", Mirror, 12 September 2015, Available from: https://www.mirror.co.uk/news/uk-news/isis-hackers-intercept-top-secret-6428423

43. Ockenden, wILL and Benjamin Sveen. "Pro-Islamic State cyber group hack websites of Australian small businesses", ABC News, 15 April 2016, Available from: https://www.abc.net.au/news/2016-04-15/pro-islamic-state-cyber-group-hack-websites-of-small-businesses/7329858

44. "ISIS-linked cyber group released kill list of 8,786 US targets for lone wolf attacks", Newsweek, 04 April 2017, Available from: https://www.newsweek.com/isis-linked-cyber-group-releases-kill-list-8786-us-targets-lone-wolf-attacks-578765

45. "ACCA claims hacking 150 twitter accounts", SITE Intelligence Group, 16 July 2019, Available from: https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/acca-claims-hacking-150-twitter-accounts.html

46. Graham-Harrison, Emma. "Could ISIS's 'cyber caliphate' unleash a deadly attack on key targets?", The Guardian, 12 April 2015, Available from: https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race

47. Ibid

48. Myers, Russell. "British hacker suspected of cyber attack on US Central Command Twitter Account", Mirror, 14 January 2015, Available from: https://www.mirror.co.uk/news/world-news/british-hacker-suspected-cyber-attack-4974855

49. Gadher, Dipesh. "British hacker is No 3 on Pentagon 'kill list'", The Times, 02 August 2015, Available from: https://www.thetimes.co.uk/article/british-hacker-is-no-3-on-pentagon-kill-list-6g95bfqwfnz

50. Meredith, Charlotte. "The Islamic State's top hacker was killed in a US drone strike", VICE, 28 August 2015, Available from: https://www.vice.com/en_us/article/neyn9x/the-islamic-states-top-hacker-was-killed-in-a-us-drone-strike

51. ET Bureau. "I have no links in the city: Mehdi Masroor Biswas", The Economic Times, 18 December 2014, Available from: https://economictimes.indiatimes.com/news/politics-and-nation/i-have-no-links-in-city-mehdi-masroor-biswas/articleshow/45556661.cms

52. "Unmasked: the man behind top Islamic State Twitter account", Channel 4 News, 11 December 2014, Available from: www.channel4.com/news/unmasked-the-man-behind-top-islamic-state-twitter-account-shami-witness-mehdi

53. Dev, Arun , Madhusoodan M.K. and Chethan Kumar, "Mehdi Biswas, IS' voice on Twitter, arrested in Bengaluru", The Times of India,14 December 2014, Available from: http://timesofindia.indiatimes.com/india/Mehdi-Biswas-ISs-voice-on-Twitter-arrested-in-Bengaluru/articleshow/45509074.cms

54. Sharma, Anurag. 2019. "The Islamic State Foreign Fighter Phenomenon and the Jihadi Threat to India. Ireland". MPhil thesis, Ireland: Dublin City University, Available from: http://doras.dcu.ie/22558/1/Anurag_Sharma_MPhil_Thesis_FINAL.pdf

55. Ibid.

56. Mehta, Ivan, "How IS Uses Social Media As A Hunting Ground For Recruits In India", The Huffington Post, 22 March 2016, Available from: http://www.huffingtonpost.in/2016/03/22/IS-uses-internet-to-rec_n_9519976.html

57. Tripathi, Rahul, "Making of a jihadi: How Mudabbir Mushtaq Shaikh became Indian face of Islamic State", The Economic Times, 09 February 2016, Available from: http://economictimes.indiatimes.com/news/defence/making-of-a-jihadi-how-mudabbir-mushtaq-shaikh-became-indian-face-of-islamic-state/articleshow/50909284.cms

58. Ibid.

59. "September 9, 2001: Internet forum message apparently warns of 9/11 attack", History Commons, Available from: http://www.historycommons.org/entity.jsp?entity=alsaha.com

60. Conway, Maura. "Terrorism and Internet Governance: Core Issues", ICTs And International Security, 2007, Available from: https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2644.pdf

61. "YouTube for Press", YouTube, Available from: https://www.youtube.com/about/press/

62. Wortham, Jenna. "A Political coming of age for the tech industry", The New York Times, 17 January 2012, Available from: https://www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?hp

63. Mekhennet, Souad. "New online magazine aims to counter extremist propaganda", The Washington Post, 05 July 2019, Available from: https://www.washingtonpost.com/world/national-security/new-online-magazine-aims-to-counter-extremist-propaganda/2019/06/04/d374f600-862c-11e9-98c1-e945ae5db8fb_story.html

64. Stanly, Johny. The ISIS Caliphate: From Syria to the doorsteps of India, (India: Bloomsbury, 2018).

65. Calamur, Krishnader. "ISIS's newest recruiting tool: regional languages", The Atlantic, 24 April 2019, Available from: https://www.theatlantic.com/international/archive/2019/04/isiss-newest-recruiting-tool-tamil-and-regional-languages/587884/

66. "Terrorism and violent extremism policy", Twitter, March 2019, Available from: https://help.twitter.com/en/rules-and-policies/violent-groups ; Tom Keatinge and Florence Keen. "Social media and terrorist financing- what are the vulnerabilities and how could public and private sectors collaborate better?", Royal United Services Institute- Global Research Network on Terrorism and Technology, Paper No. 10, 02 August 2019, Available from: https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf ; Heather Hunt. ReadKong, Available from: https://www.readkong.com/page/social-media-and-terrorist-financing-1507495