Computer Fraud and Security
ISSN (online): 1873-7056

Security Awareness for IS-Supporters on Telegram

Ala Berzinji[1*], Frzand Sherko[2], Lisa Kaati[3], Amendra Shrestha[4]

[1*]Stockholm University, University of Sulaimani, IQ Group, Stockholm, Sweden alabe@dsv.su.se
[2]The Institute of World Politics, Washington DC, USA, frzand.abdullah@iwp.edu
[3]Stockholm University, Stockholm, Sweden, lisa.kaati@dsv.su.se
[4]Mind Intelligence Lab, Uppsala, Sweden. amendra@mindintelligencelab.com

Abstract—
The so-called Islamic State (IS) has always had a strong online presence. The purpose of most IS propaganda is to shape perceptions and polarise the support of their audience, but there are also other forms of communication from the group and its supporters. In this paper, we present an analysis of the content from two IS-aligned media outlet on Telegram that specialize in cybersecurity, privacy, and encrypted communications to assist IS supporters with security awareness. We have analyzed content for a period of 60 days (from February 9th to April 9th 2022) on the first media and 180 days (from July 15th 2024 to Jnuary 15th 2025) on the second media and categorized the type of content into four different categories. Most of the communication in the channel is about cyber security awareness and tools for secure communication. However, almost 30% of the conversations are about how to secure the community, avoid detection and maintain a presence online.

I. INTRODUCTION

In 2014, the so-called Islamic State (herein referred to as IS) was successful in both creating and disseminating propaganda worldwide.

The Islamic State (IS) disseminated a wide range of content through daily radio broadcasts, photographs, videos, and text posts across various social media platforms. This content included depictions of executions, daily life within the caliphate, military operations, and religious activities. In addition to the official propaganda generated by IS, there was a significant volume of user-generated material, such as videos, poems, songs, photos, and texts, all of which contributed to the promotion of the group's ideology and activities [5], [12]. For some time, supporters of IS were active on all large social media platforms with global networks of supporters that created, circulated, and supported the spread of their messages [16].

The dissemination of IS propaganda and its resilience to removal have been likened to the Hydra, the mythical multi-headed creature from Greek mythology. Just as the Hydra would grow two new heads each time one was severed, IS propaganda often re-emerges in new forms or platforms whenever efforts are made to take it down, making it a persistent and evolving challenge [14]. The propaganda promoted in the digital arena was a significant aspect of the success IS had in recruiting followers from all around the world.

When IS lost territorial control in 2017, The group's content production capabilities were significantly weakened as a result of losing key media production facilities, essential equipment, and skilled personnel, which hindered their ability to generate and distribute propaganda effectively [6]. While IS and their fans have always been successful in promoting propaganda online, it is clear that the last couple of years has been a struggle for IS and IS fans to maintain their online networks.

Most social media platforms have increased their efforts to remove jihadis and their supporters, which makes it more difficult to communicate and distribute jihadi content online [6]. Today, jihadist groups have a resilient online presence on several different platforms including Telegram, Instagram, Facebook, Hoop Messenger, and TechHaven [8].

Telegram is one of the most important outlets for jihadis: both for official IS and 'fan' online content. The move to Telegram took place when Twitter conducted a mass account suspension of IS accounts and IS content [15]. Telegram serves as an online platform for pro-IS content with possibilities to build networks, communicate internally and a forum for recruiting new IS members [4].

While the central purpose of IS propaganda is to shape perceptions and polarise the support of their audience [9], [10] there are also other forms of communication from the group and its supporters. A growing trend involves terrorist groups leveraging privacy-enhancing tools, such as end-to-end encrypted messaging platforms, virtual private networks (VPNs), secure browsers, and mobile security applications, to evade detection and maintain operational secrecy [11]. On Telegram there are, for example, IS-aligned media outlets that specialize in cybersecurity, privacy, and encrypted communications to assist IS supporters with security awareness [7].

A. Aim

The aim of this paper is to provide a better understanding of what kind of content that is distributed on an IS-aligned media outlet that specializes in cybersecurity, privacy, and encrypted communications.

B. Outline

This paper is outlined as follows. In Section II we describe previous work on propaganda from IS. Section II describes a propaganda outlet for security awareness on Telegram.
Section IV describes the method we have used to analyze the Telegram channel and Section V presents the results of our analysis. Section VI contains a discussion of the results and finally, some conclusions and directions for future research are presented in Section VII.

II. IS PROPAGANDA ONLINE

IS propaganda has been studied from several aspects. While some research has focused on technologies for automatic detection of propaganda from IS [2], [13] others have focused more on the content of the propaganda [18], [19]. Winter [18] conducted a thematic analysis of 892 propaganda events (of which 72 percent comprised visual material) published by IS between 17 July and 15 August 2015.
The themes he examined included mercy, belonging, brutality, victimhood, war, and utopia. Among these, utopia emerged as the most dominant theme, accounting for 52.7% of the material, while war was the second most prevalent, making up 37.2% of the content. Zelin [19] systematically categorized IS propaganda into eight key variables: date, wilayat (province), country, city/village/region, media center, language(s), medium, and types. Additionally, Zelin classified the media releases into eleven distinct topics: military, governance, da'wa (Islamic missionary work), hisba (enforcement of Islamic principles), promotion of the Caliphate, enemy attacks, news, martyrdom, execution, denial of enemy reports, and other. According to Zelin, the most significant themes in IS propaganda were military operations, governance, da'wa, hisba, promotion of the Caliphate, and enemy attacks.
As previously noted, Telegram has become one of the primary platforms for IS supporters' online communication. Its use by IS is frequently highlighted in media reports as evidence of a new era in jihadist online activities, marking a significant shift in how such groups disseminate their messages and coordinate operations [4]. In a study of how IS use Telegram [4] it was noted that some of IS Telegram channels shared information about general cyber security practices when accessing and communicating on Telegram. To obscure any potentially identifying information, users were suggested to employ basic cyber security measures. Instructions on how to use VPNs, create fake Telegram accounts and phone numbers, and adopt privacy software, are frequently shared within these networks to help users maintain anonymity and avoid detection. are distributed in proIS Telegram channels.
The rest of this paper is focused on two IS-aligned Telegram channels that focuses on providing members and supporters with information about security awareness.

III. IS-ALIGNED OUTLET FOCUSING ON SECURITY AWARENESS

We have analyzed two Arabic language channels on Telegram. Both channels can be described as an IS-aligned outlet for security awareness. To avoid getting shut down, the administrators of the channels provide instructions to the members to the members on how to communicate, and some of the communication in the channel is also encrypted. In the early days of the channels, the encryption was done manually by splitting certain words (a list of blacklisted words are provided in the channels) and then inserting spaces or dots between the characters in various ways. Later, the administrators of the channels provided a software program to encrypt certain words by inserting spaces or dots between the characters and also adding English numbers and characters to the Arabic words.
The encryption is probably one reason why the channels is still active during a time when Telegram shuts down hundreds of channels and accounts for violating their terms of usage. When communicating on the channels, the users are provided instructions not to use language, symbols, pictures, videos, or news that can be linked to IS. The channel administrators provide the users with an encryption method that changes words related to ideology or terrorism either manually or via an automated process.
Some of the activities that take place on the channels are:

- Distribution of instructions on how to act online to avoid detection of authorities.
- Information about tools that can be used to have a secure presence online.
- Instructions on how to avoid viruses and malware to prevent being hacked.
- Instructions on how to act if you get hacked.
- Information about how to obtain new phone numbers using different kind of software

IV. METHOD

The data we have used is downloaded from both channels on Telegram. The channels are open, and it does not require membership to read the communication. The first channel, on April 9th 2022, the channel had 799 members and three administrators. The data consists of 5 000 posts published between February 9, 2022 and April 9, 2022, The posts include 309 links, 80 pictures, 11 files, and 4 video clips. The second channel, on July 15th 2024, the channel had 1540 members and four administrators. The data consists of 23 000 posts published between July 15, 2024 and January 15, 2025, The posts include 2600 links, 80 pictures, 11 files, and 4 video clips.
To get an understanding of the content on the channels, we have done a content analysis. As a first step, we read through part of the material. As a second step, we created a set of categories with the concepts that were prominent in the data.

The different categories that we identified were:

- Community-related communication
- General security awareness
- Cyber security awareness
- Offensive and defensive hacking

A. Community-related communication

Community-related communication is communication that contains instructions and information on how members of the community should behave. To maintain a presence on Telegram, members of the channel are instructed not to use words and terms that may attract the attention of companies and intelligence agencies to either the individual members of the channel or the channel itself. The members of the channel are instructed not to use Arabic words for ”Islam,” ” jihad,” ”Islamic state,” ”supporting Islam and jihad,” ”war,” and ”brotherhood,” as well as words such as ”security”, ”government”, ”intelligence”, ”hacking”, and ”cyber.”

To avoid that members accidentally use some of the forbidden words, there is a software program that automatically scans all communication on the channel. If a blacklisted word is detected, the message is deleted. There is also a possibility for the members to encrypt their communication manually either by replacing certain words or by changing some of the Arabic letters by Latin letters, numbers, and symbols.

Another part of the messages in this category is to instruct members to follow the guidelines of Electronic Horizon Foundation (Afaq). Afaq was established around 2016 and aligned itself with the Islamic State Caliphate. Afaq provides online users with tools to prevent surveillance, tips on cyber security, warnings against the use of certain apps, websites, and fake social media accounts [3].

B. Cyber security awareness

This category contains messages that contain general guidelines on cyber security. For example, information about new technology, cyber security, and potential threats.

Part of the communication contains recommendations and requests. Here, members ask for advice regarding what tools they should use and also recommendations of tools that they have used successfully.

Other messages contain information about new technology and also about potential threats. The members of the channel are encouraged to learn how to protect themselves before engaging in operations that support any of IS activities. The importance of avoiding detection by law enforcement as well as the large social media companies is emphasized in the communication.

A large part of the security awareness communication consists of advice about what VPN:s that are good to use. The communication also contains information on how to create virtual numbers, how to hack accounts in Telegram and Facebook, tools for storing confidential information in iCloud, and tools for spreading propaganda without being detected.

C. Offensive and defensive hacking

The category offensive and defensive hacking contain messages related to hacking. Some messages are about hacking pages and accounts of perceived enemy groups, anti-religious groups, or supporters of a liberal lifestyle. Other messages are about attacking governments and security agencies.

D. General security awareness

This category includes messages that are not related to cyber security but to general security. This is, for example, communication about physical security, counterintelligence, and how to conduct attacks and avoid being detected. Members of the channel share experiences about working undercover and explain guidelines and working methods.

V. RESULTS

The distribution of the different categories is shown in Fig.1. As can be seen, the largest category is Cyber security awareness (64.46% of the messages) followed by Community related communication (25.71% of the messages). Offensive and defensive hacking and general security awareness are smaller categories with 6.67% and 3.18% of the messages.

The largest part of the communication in the channel is about cyber security awareness. This kind of communication is about tools and techniques for cyber security. In particular recommendations on what kind of tools that should be used.

TABLE I DIFFERENT TOOLS AND APPS THAT ARE RECOMMENDED FOR USAGE.

VPNs	Other tools
Lilac VPN	Proton mail (email)
Bitmask	Temp mail (email)
Solo VPN	TextMeUp (create multiple numbers on your phone)
VPNhub	Avast (antivirus)

Windscribe	Onionshare (file sharing)
Hide.me	StegHide (steganography)
Canada VPN	ESET (antivirus/security)
Turbo VPN	2ndLine (second phone number)
CyberGhost	Cryptocurrency (Monero)
Proton VPN	SafeUM (secure instant messenger)
SoloVPN	FreeTone (free calls to the US and Canada for both landlines and cell phone)
NordVPN	MEGA (cloud storage)
Mullvad	Onion Routing (anonymization method)
ExpressVPN	Secure OS (Tails OS)
FastVPN	ExifTool as a powerful tool, it allows users to read, write, and edit metadata in a various file formats
Orbot	Talkatone (call and text communication app)
RiseupVPN	NewPipe (app for watching YouTube, PeerTube and other media platforms)

Table I shows some of the tools that are recommended. Most of the tools that are discussed are VPN:s. When using a VPN you encrypt your internet traffic and disguise your online identity. By using a VPN it is more difficult for third parties to track your activities online. Other tools that are mentioned in the channel are tools for obtaining several phone numbers, tools for making free calls, cloud storage, antivirus tools and tools for secure communication using emails or text messages.

A total of 1450 messages are concerned with community related communication. Out of these, almost half of the messages (700 messages) are about words that are forbidden to use openly in the channel and how these words should be encrypted.

VI. DISCUSSION

on the both IS-aligned media outlet that we have analyzed, most of the communication is concerned with cyber security awareness (64.46%). This kind of communication includes general advice as well as specific recommendations for tools that can be used. The list of tools in Table I shows that while most focus is on different VPN:s many other tools are also recommended.

Almost 25% of the communication is community-related. The main purpose of this kind of communication is to ensure that the members of the channel communicate in a way so that removal from Telegram is avoided. A large part of the messages (40% of the community-related messages) in the category community-related communication is about encryption of communication and in particular certain words that are believed to attract the attention of Telegrams moderators. This indicates that the focus of the IS-aligned media outlets is not only to assist IS supporters with security awareness but also to maintain a presence on Telegram and avoid shout-downs.

Less focus is put on general security awareness (such as physical security) and on offensive and defensive hacking.

VII. CONCLUSIONS AND FUTURE WORK

The focus of this paper has been to describe and analyze propaganda from two IS-aligned media outlets that specialize in cyber security, privacy, and encrypted communications to assist IS supporters with security awareness. By learning more about what kind of communication that is present in IS-aligned media outlets we can learn more about how IS continues its actions to support online jihad despite intense international pressure from governments and private companies.

Digital propaganda has always been an important part of IS's successes, and the organization and its followers have been successful in producing, targeting, and disseminating propaganda that above attracts individuals from different countries and age groups [5].

Many of the major social media companies have dedicated significant effort and resources to removing IS propaganda from their platforms. However, removing all IS propaganda from social media is difficult since IS also use several anonymous sharing portals to disseminate their propaganda [17].

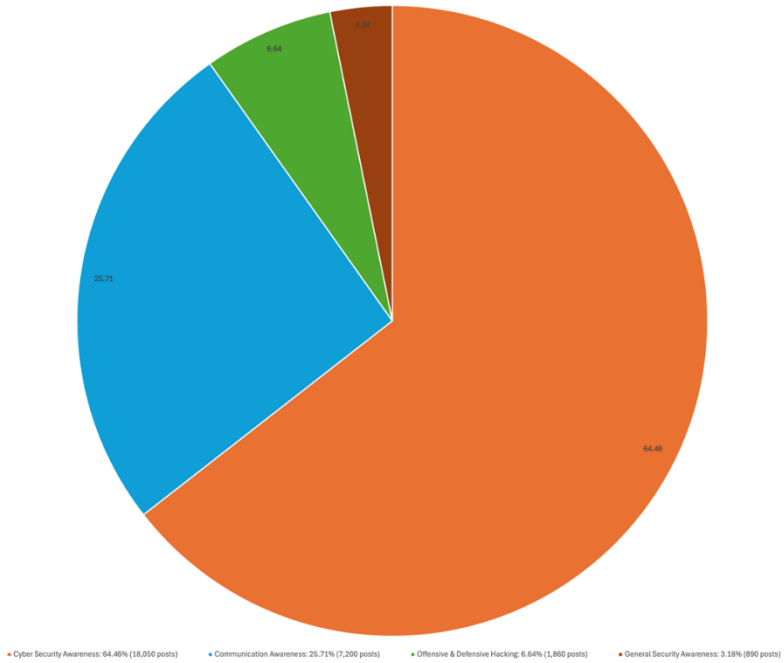

Fig. 1. Distribution of the different categories

With the loss of the physical caliphate, today's IS supporters rely heavily on the Internet which also requires that the supporters have knowledge of cyber security and security technologies for escaping surveillance and maintaining a presence online [1].

For future work, it would be interesting to identify more ISaligned media outlets that focus on cyber security awareness and conduct a larger study on who these channels operate to maintain a presence online as well as what kind of tools that are recommended to their members.

REFERENCES

[1] L. Alkhouri and K. Alex. Tech for jihad: Dissecting jihadists' digital toolbox. *Flashpoint*, 2016.
[2] M. Ashcroft, A. Fisher, L. Kaati, E. Omer, and N. Prucha. Detecting jihadist messages on twitter. In *2015 European Intelligence and Security Informatics Conference*, pages 161–164, 2015.
[3] E. Azani and D. Haberfeld. The end of the islamic state's cyber security unit afaq? International Institute for Counter-Terrorism (ICT), 2022.
[4] B. Clifford and H. Powell. Encrypted extremism: Inside the englishspeaking islamic state ecosystem on telegram. GW Program on Extremism, 2019.
[5] K. Cohen and L. Kaati. Digital jihad. propaganda from the islamic state. Swedish Defence Research Agencey. FOI-R–4645–SE, 2018.
[6] M. Conway, A. L. Watkin, and S. Looney. Violent extremism and terrorism online in 2021: The year in review. European Union, 2021.
[7] Europol. Online jihadist propaganda - 2020 in review. Publications Office of the European Union, Luxembourg, 2021.
[8] Europol. Online jihadist propaganda 2021 in review. Publications Office of the European Union, Luxembourg, 2022.
[9] H. J. Ingram. The strategic logic of islamic state information operations. *Australian Journal of International Affairs*, 69(6):729–752, 2015.
[10] H. J. Ingram. Learning from isis's virtual propaganda war for western muslims: A comparison of inspire and dabiq. Terrorists' Use of the Internet: Assessment and Response., 2017.
[11] H. J. Ingram. "that is what the terrorists want": Media as amplifier or disrupter of violent extremist propaganda. ICCT, 2017.
[12] L. Kaati. Det digitala kalifatet. en studie av islamiska statens propaganda. Swedish Defence Research Agencey. FOI-R– 4429–SE., 2018.
[13] L. Kaati, E. Omer, N. Prucha, and A. Shrestha. Detecting multipliers of jihadism on twitter. In *2015 IEEE International Conference on Data Mining Workshop (ICDMW)*, pages 954–960, 2015.
[14] C. Picart. "jihad cool/jihad chic": The roles of the internet and imagined relations in the self-radicalization of colleen larose (jihad jane). *Societies*, (5.2):354–383, 2021.
[15] N. Prucha. Is and the jihadist information highway – projecting influence and religious identity via telegram. *Perspectives on Terrorism*, 10(6):48– 58, 2016.
[16] C. Schori Liang. Cyber jihad: Understanding and countering islamic state propaganda. GCSP Policy Paper, 2015.

[17] A. Shehabat and T. Mitew. Black-boxing the black flag: Anonymous sharing platforms and isis content distribution tactics. *Perspectives on Terrorism*, 12(1):81–99, 2018.
[18] C. Winter. Documenting the virtual 'caliphate.'. Quilliam Foundation, 2015.
[19] A. Zelin. Picture or it didn't happen: A snapshot of the islamic state's official media output. *Perspectives on Terrorism*, (9), 2015.