An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom

Victoria Jangada Correia¹

Received: 28 September 2021 / Accepted: 4 November 2021 / Published online: 24 November 2021
© The Author(s) 2021

Abstract

Terrorism, crime, and war are all familiar notions; however, the way in which these have been altered through cyberspace is not yet fully, nor unanimously, understood through definitions, theories, and approaches. Although the threat level of terrorism in the UK has lowered to moderate, the threat posed by cyber terrorism has nonetheless heightened throughout the COVID pandemic due to the greater necessity and presence of technology in our lives. This research aimed to highlight the necessity for a unanimous cyber terrorism definition and framework and further aimed to determine what perceptions are held by the general public regarding cyber terrorism through a mixed methods approach. The literature review confirms that there is an absence of a unanimously agreed upon definition of cyber terrorism, and furthermore that the existing academic definitions are not compatible with UK legislation. In addition, the literature review highlights an absence of a cyber terrorism framework that classifies what kind of terrorist activity is cyber enabled or cyber dependent. Quantitative data from the online survey find a couple of significant effects implying the necessity for greater diversity amongst stakeholders which could potentially enhance the detection and prevention of terrorism in the UK. The qualitative data find that although there is some agreement amongst the sample population in views held towards cyber terrorism, some misconceptions are nonetheless present which could have implications on the general public's ability to identify and report cyber terrorist activity. Overall, the findings from the literature review and the primary data collection aid in developing a cyber terrorism definition that is compatible with UK legislative definitions, and further aids in developing a terrorist activity framework that succinctly highlights the inextricable links between traditional, cyber enabled, and cyber-dependent terrorism.

Keywords Cyber terrorism · Counter terrorism · Cyber crime · Policing

Introduction

Overview of Research

For almost up to 2 decades, the search for defining cyber terrorism has been described as the 'Holy Grail' for scholars and policy makers [1]. This has been escalated during the recent COVID pandemic where life has made a remarkable

shift towards online activity, placing individuals at a much higher risk of being vulnerable to cyber terrorist activities [2]. Although there has been considerable research focusing on how cyber capabilities facilitate terrorism [3–5], there is nonetheless significant disagreement surrounding what definitions and approaches should be used unanimously to facilitate in preventing, detecting, investigating, and prosecuting cyber terrorist threats by key stakeholders in the United Kingdom (UK) such as the police, prosecution services and policy makers and international stakeholders too.

This disagreement could be due to the notion that cyber terrorism as a term, houses a wide range of illicit behaviours including hacking and phishing, to sharing online propaganda, radicalising and recruiting individuals. Therefore, attempting to define everything under the term 'cyber terrorism' can become challenging due to legal contexts, objectives of the illicit behaviour, and intent [6]. The lack of a unanimous definition has further delayed a framework

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest-edited by Rajiv Misra, R K Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ Victoria Jangada Correia
vickyalexc@icloud.com

¹ School of Criminology and Criminal Justice, University of Portsmouth, University House, Winston Churchill Avenue, Portsmouth PO1 2UP, UK

for cyber terrorism being developed. McGuire and Dowling [7] coined the cyber-dependant and cyber-enabled cyber-crime classification; however, cyber terrorism was outside the scope at the time, and this has not been further reviewed to date.

As at financial year end on March 2020, 261 arrests of terrorism-related activity were recorded [8]. However, as at financial year end on March 2021, there was a 37% reduction in terrorism-related arrests [9]. Not only are these statistics potentially reflective of the three national lockdowns and restrictions put in place for the COVID pandemic but are also potentially indicative of terrorist activity transitioning further into online platforms and not being regulated effectively. It was found that in the middle of the pandemic, terrorist groups had been altering their methods of sharing their beliefs through a plethora of online platforms, from disseminating propaganda to spreading misinformation and conspiracies to attain further support [2]. These findings highlight a socio-technical perspective in which the inextricable links between terrorist technological use and its impacts on society are evident. This perspective highlights the need for a more collaborative approach from stakeholders to create greater security for society from terrorism.

Interestingly, the aforementioned issues are also prevalent and long-standing in the taxonomy of cybercrime and the crimes which are included under this term [10–12]. This alludes to widespread conflict in the foundational understanding of cybercrime as a whole which inevitably affects the approach to counter cyber terrorism. Therefore, the rationale for this research highlights the importance of law enforcement, policy makers and prosecuting services having a clear definition and framework for cyber terrorism and its links to traditional terrorism, allowing them to combat the threat collaboratively. However, it is perhaps important to note that recent research found that the use of nonspecific interventions to deter terrorist activity could in fact lead to an increase in terrorist attacks [13]. In light of this, more specific interventions and a clearer understanding of underlying criminal behaviours are necessary to effectively combat the threat of terrorism, further highlighting the need for a more unanimous and concise definition and approach from relevant stakeholders in countering cyber terrorism.

Research Aims and Objectives

This research primarily aims to establish a concise definition of cyber terrorism and a suitable framework that clearly elaborates on terrorist and cyber terrorist activity to be considered by UK stakeholders. In order to achieve this primary aim, this research's research will investigate and critically analyse the etymology of the words so to better understand the term 'cyber terrorism'. Furthermore, current definitions of terrorism and cyber terrorism will be reviewed and

analysed to determine the strengths and weakness of viewing cyber terrorism in certain ways. Additionally, Space Transition Theory [14] and Routine Activity Theory [15] will be analysed to inform a discussion on cyber terrorist behaviours and processes. Lastly, the Smith et al. terrorist group activity process [16] will be analysed alongside the McGuire and Dowling [7] dual binary classification, to support the development of a proposed framework.

This research then aims to determine what the public's perceptions are towards cyber terrorism as this could be representative of bigger issues regarding misconceptions on the topic. To conduct a reasonable investigation, this research will collect quantitative and qualitative primary data by means of an online survey. The data will first be statistically analysed to determine any significance between participant demographics and opinions. The data will then be thematically analysed to determine any strong themes which relate to participant opinions and identify common views held by the sample population in context of the findings from the literature review.

Article Layout

The structure which this research will follow includes a literature review where relevant literature, definitions, and frameworks will be evaluated to present a clear outline on what the current state of defining cyber terrorism is. This will be followed by a methodology chapter which will discuss and analyse the mixed methods approach adopted for this research's primary data collection. Subsequently, the quantitative and qualitative results will be interpreted in the context of the findings from the literature review, with analysis of the implications and limitations of the data. Within the results and findings chapter, a new cyber terrorism definition and framework will be proposed and analysed. Finally, the research will offer conclusions and recommendations highlighting how the study could be improved and further researched.

Literature Review

Modern Day Understanding of Terrorism

Defining terrorism is a subject matter undergoing much discourse [17–19]. This struggle in defining terrorism could be attributed to the difficulty in reflecting ideological, philosophical, political and religious normative differences under a single term. As a result of this, further confusion can become apparent in justifying the legality or illegality of suspected terrorist activity. Terrorism has been depicted as a social construct as the meaning of it is shaped by the

views held by the person categorising what terrorism means to them [20, 21].

According to Hewer and Taylor, the term terrorism is merely a marker used by governments to legitimise or delegitimise politically motivated violence occurring in their country [22]. A good example of this is the paradoxical nature between the Middle East and the West in their characterisation of terrorism. In the Middle East there is an amalgamation between religious identity and politics which influences societal and cultural concepts directly [23, 24], whereas in the west there is a strong distinction between religion and politics resulting in a democratic society which enables an array of societal and cultural ideals to cohabit [22, 25]. The beliefs and ideologies held by the West and the Middle East see one another as a threat to their respective core norms and values which is potentially where the notion of terrorism emerges [26, 27]. Overall, this information emphasises the belief that different countries may have different meanings of what qualifies as a terrorist act or not depending on their political and religious alignment. In light of this, it is important to acknowledge that the prosecution of a terrorist who is not based in the UK may be troublesome due to these differing aspects, especially with cyber terrorism where threats or acts of violence and disruption can be communicated or committed through cyber capabilities off British soil.

The Terrorism Act 2006 [28] and The Counter-Terrorism Act 2008 [29] are amongst some of the acts which detail illicit behaviours within terrorist activity. More specifically, The Terrorism Act 2006 defines terrorism as an act, or threat of act of violence against the public and/or property, to intimidate the public and/or property, or to advance political or religious ideologies. This definition has been criticised due to its implications on principles of legality and its lack of clarity in defining what actions are ascribed as ‘terrorist’ which may mislead public and political perceptions regarding terrorism [18, 21]. This vagueness could be attributed to confusing wording within legislation, which could further cause individuals engaging in terrorist activity to not be aware of the illegality behind their behaviour. Regardless of these downfalls, it is important to consider the UK’s legislative definition of terrorism in this literature review as it is pertinent that any future cyber terrorism definition be compatible with already existing legislation.

Media coverage has also contributed massively to the way in which terrorism is defined and understood and have blurred the lines between victims and perpetrators of terrorist acts [30]. The media’s use of terms such as ‘freedom fighting’, ‘insurgency’ and ‘extremism’ has caused the foundational meaning of terrorism to be replaced and misunderstood [18]. As a result, the original understanding of the term terrorism has been modified to suit the many political and religious terrorist organisations operating in modern

society. This could potentially result in news media outlets shaping and promoting misconceptions amongst public opinion.

This can be better understood through Gatekeeping Theory which explores the way in which information is selected and disseminated to a group of people by news media outlets [31–33]. Shoemaker and Vos [32] further developed the theory, specifically investigating the way in which information of an event is passed through a series of ‘gatekeepers’ who determine what information will be disseminated, how and to whom. This theory challenges one to consider how the gatekeeping process may potentially wittingly or unwittingly distort the general public’s understanding of terrorism and terrorist activity according to the differing political, religious, or societal alignments held by news media outlets. In light of these findings, it is clear that a unanimous understanding of terrorism should be shared across the various stakeholders to improve the accuracy of the information being shared to the public.

Understanding the ‘Cyber’ Prefix

The term ‘cyber’ as we know it today originates back to *kebernetes* which was an ancient Greek phrase which translates to ‘the art of steering’ [34]. It was not until mathematician Norbert Wiener used the word *cybernetics* in the 1940s that the term came to be known as a study of the systems within living beings and artificial machines [35]. This term was further influenced by pop culture in the 1980s during the cyberpunk movement which was inspired by William Gibson’s novel *Neuromancer* [36], which further associated the ‘cyber’ term with dystopian and futuristic concepts. At a similar time to this, there had also been a shifting approach and understanding within the US military with regard to information warfare and the changing nature of the modern battlefield [37].

Flutter argues that the cyber prefix is nothing but a catch-all phrase which has resulted in a term that has been overly ill-defined due to the various range of factors which it tries to explain [38]. In his article, Flutter suggests that returning the terms ‘Information Warfare’, ‘Information Operations’ and ‘Computer Network Operations’ instead of the cyber prefix would be more beneficial as this would clearly classify crimes which are dependent to technology. Conversely to this view, it has been argued that a definition of cyberspace should not be solely categorised under the technological components as “cyberspace allows the exercise of power” [39]. Although Computer Network Operations as a term has mostly been used in warfare, there have yet been implications to push this into the broader scope of cybercrimes.

It could be useful to apply the above terms to terrorism rather than the cyber prefix as this could more clearly define terrorist activity which is fully dependent on technological

capabilities such as denial of service attacks. This approach to focus on the computer and information operations has been adopted by a few academics in their definitions of cyber terrorism [40, 41]. However, such an approach is arguably limited as it excludes other types of terrorist activities which are being enabled by other aspects of technology such as the dissemination of terrorist propaganda and recruitment. Although separate terms could be designed to distinguish between these differing approaches to terrorist activity, the cyber prefix has become a synonymous catch all phrase distinguishing between traditional crimes and more modern crimes being committed through technological capabilities. In light of this, a term such as ‘computer network operations’ or ‘information warfare’ may not be suitable to further explore and define cyber terrorism as these terms overlook other types of terrorist activity. In turn, this would reject the inextricable links between technology, terrorism, and their impacts on communities, not just computer networks. Therefore, this literature review proposes that the use of the cyber prefix is pertinent for a clear and synonymous categorisation between traditional terrorism and cyber terrorism.

Current Definitional Interpretations of Cyber Terrorism

Cyber terrorism definitions are mostly based upon traditional terrorism definitions such as the aforementioned. It has been suggested that attacks can qualify as cyber terrorism if there is intent to impede on the political, social, or economic functioning of a group, organisation or country, or to provoke/perpetrate acts of physical violence [42]. Holt further supports this definition by suggesting that the term cyber terrorism should encapsulate the behaviour leading to the act, without necessarily resulting in physical disruption or damage [43]. Both these definitions put emphasis on the intent and motivations behind cyber terrorist activity instead of narrowly focusing on the physical impacts.

Conversely, other academics have taken a different stance on the matter and have argued that to qualify an attack under cyber terrorism, physical damage and/or disruption against a computer or network must occur [40, 41]. Despite efforts made by academics to define cyber terrorism, some have further argued that the cyber prefix to terrorism only elaborates on the method employed in committing terrorism and therefore ‘cyber terrorism’ does not require its own category [44]. As technology continues to evolve and becomes more accessible, viewing cyber terrorism as proposed by Gordon and Ford [44] and Denning [41], could pose a greater risk to public safety, as well as impact law enforcement’s understanding and approaches in preventing, detecting, and investigating cyber terrorist activity.

These cyber terrorism definitions offer differing insights into what may and may not qualify as cyber terrorism, but it

is important to acknowledge the dates when these definitions were conceived. As technology has significantly evolved since the conception of these definitions, it has become necessary to agree upon an up-to-date cyber terrorism definition that incorporates all aspects of modern technology. A more recent study was conducted identifying the key characteristics present in an array of cyber terrorism definitions to establish a new definition based off of these components and the study concluded that [45]:

“Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace to cause real world consequences in order to influence fear or coerce civilian, government, or non-government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychological, political, economic, ecological, or otherwise that occur outside of cyber space.”

This definition emphasises the actor, motivation, intent, means, effects and targets of cyber terrorism. Comparing this definition to those by Foltz [42] and Holt [43], there are some similarities; however, this definition puts further emphasis on the effect of the cyber terrorist activity which is pertinent to better understand what kind of acts actually encapsulate cyber terrorism. In comparison to the definitions proposed by Denning [41] and Conway [40], the Plotnek and Slay [45] definition does not only focus on cyber terrorist activity which may have physical impacts, but also focuses on other effects such as psychological and economic. This is an important aspect in defining the cyber terrorism term as it acknowledges all impacts which technological platforms are having on terrorism and subsequently on communities, rather than just a singular aspect. Although important points are covered in this explanation of cyber terrorism, it is nonetheless a long-winded definition with many different clauses which may not be simply understood. Furthermore, Plotnek and Slay are Australian based researchers and therefore the applicability of their definition to UK legislation is perhaps dubious due to its lack of compatibility with the current definition of terrorism outlined in The Terrorism Act 2006 [28]. A more suitable approach to defining cyber terrorism more succinctly, could be to divide it into clearer themes and shorter sentences.

Realistically, cyber terrorism is a very broad topic, and a definition which may endeavour to cover all the characteristics which fall under this term is seemingly challenging. Therefore, the attempt to encapsulate every aspect of cyber terrorism under one singular definition may be counter-productive and may potentially be the very notion preventing a unanimously agreed upon definition. Furthermore, there seems to be a lack of compatibility of the above definitions with the UK legislative definition of terrorism, therefore, a

cyber terrorism definition could be designed in the context of UK law.

Theoretical Underpinnings of Cyber Terrorism

Terrorists use cyber space for an array of activities including hate speech, propaganda, recruitment and communication [46]. This literature review found that Routine Activity Theory [15] and Space Transition Theory [14] can be applied to cyber terrorism to support a clearer understanding behind the motivations of cyber terrorist offenders, in turn aiding stakeholders in the prevention, detection, investigation and prosecution of cyber terrorism.

Routine Activity Theory

Routine Activity Theory was developed by Cohen and Felson in 1979 and proposed that in order for there to be an occurrence of victimisation, three confluent factors were necessary: first, a motivated offender; secondly, a suitable target; and thirdly, the absence of a capable guardian. When this theory is applied to cybercrime, the notion of physical space is modified into cyberspace [47–49]. A study was conducted into the relationship between university students and their computers, and it was found that students who had a greater tendency to disregard their computer-oriented lifestyles and/or neglected security software on their computers, were more likely to be victims of computer crimes [47]. This study highlights a moderation to the original routine activity theory by which the absence of a guardian may not only be a physical person but could also be the lack of security software on a victim's technological device.

Although this study was specifically about hacking, the cyber routine activity theory has nonetheless been applied to other forms of cybercrimes [50] and these findings can be applied to cyber terrorism to better illuminate the three confluent factors in relation to online terrorist activity. For example, if there is no computer security or blocked websites, this could enable the motivated offender to carry out a threat or act of terrorist violence against a suitable target.

Space Transition Theory

Space Transition Theory, created by Jaishankar [14], was developed to better explain the transitioning of cyber-criminal behaviour between physical space, to cyber space and vice versa. This theory explores seven main tenets: (1) propensity to commit cybercrime as a result of repressed offline criminal tendencies; (2) flexible identity within cyber environments; (3) freedom to transition between physical and cyber spaces; (4) criminal opportunity with little regulation and chance of being caught; (5) offenders' social connections; (6) reduced threat to offenders; and (7) the blurred

lines between norms and values within cyber environments. The principles within Jaishankar's [14] theory provide greater comprehension in the paradoxical characteristics between traditional and cybercrimes, and three of these can specifically contribute to better understanding cyber terrorism.

Firstly, due to the anonymous nature of cyberspace, there is a straightforward opportunity for cyber terrorists to disguise their identity, previously referred to as dissociative anonymity [50, 51]. This anonymity enables terrorists to hide their identity as a way to bypass existing regulations within cyber environments. Second, due to the anonymous nature of cyber environments, this not only impacts how actions can be regulated, but also allows offenders to continue their criminal behaviour with little to no consequences. This is further supported by cognitive inhibition effect in which, due to lack of deterrence, dissociation between the action and the end result encourages the continual terrorist behaviour [50]. Third, the ability to interchange between physical space and cyber space, alludes to the notion that terrorist activity may potentially manifest in cyber space where there are limited constraints to disseminate propaganda and recruit, prior to moving into physical space where offline impacts may be seen [52]. This available interchangeability is financially advantageous to terrorist groups as they can achieve their aims and objectives to further their terrorist ideology with reduced monetary costs.

Lastly, if terrorist behaviour is repressed in physical environments, this may encourage terrorists to modify their approaches into cyberspace where activities can be hidden from regulatory bodies and stakeholders involved in combating terrorism [53]. Although this was an already advantageous aspect for terrorists, this has become even more significant due to the global COVID pandemic and lockdown restrictions [2]. Due to a greater increase in terrorist use of cyber space and its dynamic spatial-temporal characteristic, there is a lower risk of being caught due to the vastness of cyber environments [52]. Overall, the tenets highlighted in Space Transition Theory [14] simplify the advantageous elements which are enabling terrorist activity to continue mostly uninterrupted.

Categorisation of Cyber Terrorist Activity

According to the Crown Prosecution Service [54], in order for an action to qualify as terrorism, there needs to be evidence of terrorist motivations. Wilkinson identifies four types of terrorist groups: ethno-nationalist groups; ideological groups; religio-political groups; and single-issue groups [55]. This identification can be used to inform the types of motivations which can influence terrorist offences. The current legislations for countering the threat of terrorism in the UK are The Terrorism Act 2000 [56]; The Terrorism Act

2006 [28]; The Counter-Terrorism Act 2008 [29]; and The Counter-Terrorism and Border Security Act 2019 [57].

According to the Crown Prosecution Service [54], some examples of substantive terrorist offences include preparing terrorist attacks; collecting terrorist information; disseminating terrorist publications with intent of encouraging terrorism; aiding in covering up terrorist activity online; supporting a proscribed organisation; attending a place for terrorist training; and financially aiding terrorist activity. In the context of the above offences, one could question the effectiveness of current UK legislation in preventing, detecting, investigating and prosecuting cyber terrorist activity. For example, the offence of ‘attending a place for terrorist training’ under The Terrorism Act 2006 [28] may be challenging to apply to terrorist virtual training as there is no geographic “place” due to the boundaryless characteristic of a cyber environment. Both pinpointing the virtual location of training and determining the IP addresses of each individual attending the training session, could make it difficult for stakeholders to detect and prosecute [58, 59]. However, as explored in Space Transition Theory [14], this is an advantageous notion for cyber terrorism due to the anonymity factor. In addition, it is important to note that terrorist activities, such as training and recruitment, have become more reliant on online platforms, especially throughout the COVID pandemic due to restrictions.

Recently, The Department for Digital, Cultural, Media and Sport [60], released a Draft Online Safety Bill which aims to set out principles for service providers in regulating their services and making them safe for users. It directly highlights principles which should be used to combat online terrorist activity. The draft bill has been under scrutiny for the risk it poses to freedom of speech, privacy and the way in which it will regulate risks to the public [61, 62], however, it is nonetheless a step in the right direction to continue combatting the threat posed by terrorism in the UK. Although UK laws can be a beneficial tool in understanding what offences can be prosecuted, it is limited in clearly categorising terrorist offences and their processes in a framework approach.

Smith et al. [16] conducted a study into the spatial and temporal patterns of terrorist group activity, and although classifying terrorist activity was not a main aim, this was nonetheless achieved and can be used to better understand terrorist processes. This study breaks down terrorist activity into four main categories: (1) recruitment; (2) preliminary organisation and planning; (3) preparatory conduct; and (4) terrorist act. This framework can be useful in gaining a clearer understanding of what general types of terrorist activity occur and, furthermore, how one act can lead to another. This could be a beneficial tool for stakeholders involved in the prevention, detection, investigation, and

prosecution of traditional and cyber terrorism as there would be a clearer understanding of the entailed processes.

McGuire and Dowling developed a dual-binary framework approach which classifies cybercrimes based off their dependence to cyber capabilities [7]. Cyber-enabled crimes, such as disseminating terrorist propaganda or theft, are traditional crimes which can increase in scale due to technology. On the other hand, cyber-dependent crimes, such as denial of service attacks or hacking, are acts which can only be committed through technological means. This dual binary approach is beneficial as it encourages a clear classification which can be easily understood by direct stakeholders such as law enforcement and prosecution services. However, this approach is limited as it does not apply this model to cyber terrorism [7]. Considering this approach has been adopted by the Crown Prosecution Service [63] to better explain the prosecution of cybercrimes, this could be indicative of a lack of understanding towards cyber terrorism from the criminal justice system in the UK. This raises a critical question of whether the criminal justice system is suitably equipped with knowledge in securing the UK against the threat posed by cyber terrorism. Considering the rise of online based terrorism throughout the pandemic [2], a dual binary approach may not be sufficient, but rather a ternary approach which incorporates traditional, cyber enabled and cyber dependent terrorism, could instead be considered to enhance the understanding of varying terrorist activities and their correlations.

Methodology

Research Design

In order to determine what perceptions were held by the public towards cyber terrorism, a mixed methods approach was chosen over a single method approach as mixed methods enable the researcher to find comparisons and contradictions within the quantitative and qualitative data which overall strengthens the discussion to better understand something, which as highlighted in the literature review, is not yet well understood [64, 65]. By utilising a mixed methods approach, quantitative and qualitative data were collected and analysed simultaneously using positivist (quantitative) and post-positivist (qualitative) paradigms to observe and measure the responses [66, 67].

Research Materials

The research material used was a mixed methods questionnaire which consisted of both quantitative and qualitative questions in the form of an online survey which was open to the public. Some benefits of utilising surveys to collect data are that participants are able to answer questions in their own

time, and furthermore can answer truthfully without a fear of being judged as they are in a familiar environment [68, 69]. Also, online surveys have been found to be beneficial as they are simple to implement and inexpensive compared to traditional questionnaire characteristics such as printing, postage, location and time [70, 71].

The online survey was created through Jisc Online Surveys [72] which was used to create and host the survey for participants to complete the questions using a link. It was important to the research that the survey be made simple for ease of participants to navigate through it themselves and, therefore, where needed, explanations were put in place to aid participants throughout the survey. The survey used a range of demographic questions, dichotomous questions, Likert scale questions, and open questions. Every question gave respondents the opportunity to elaborate on their responses with free text boxes which fed in to the qualitative data.

Participants were specifically asked questions regarding their beliefs towards the way in which cyberspace is enabling terrorism. Participants were asked to share what threat level they believe the UK currently faces from terrorism and were also asked their opinion on the importance of stakeholder's understanding to improve the UK's approach to counter cyber terrorism. The questions under this section made up an important part of this research as they directly correlated to the aims and objectives. This enabled the analysis against the demographic groups to be done to ascertain what the sample populations' perceptions were towards cyber terrorism.

Research Sampling and Procedure

The sampling techniques which were dedicated to this research were convenience sampling and snowball sampling. The convenience sampling method does not rely on probability and takes a sample from a group of people who meet a certain criterion [73, 74], where for this research the criteria were easy to reach; availability; and over the age of 18. A limitation of convenience sampling is that it encourages biased results due to the potential proximity of the researcher and the respondents and therefore, opinions in the data may not have the ability to be fairly applied to the general population [74, 75]. In light of this limitation, the snowball sampling method was then also utilised by encouraging respondents to share the survey once they had completed it to at least one other person as this would increase the sample size and generalisability of the data [76]. This would ensure that the sample was more diverse.

The online survey was distributed through a web link which was shared via the researcher's social media accounts with a short explanation of the research so that participants could make an informed decision of whether they wished to participate or not. The social media sites used included

LinkedIn; Facebook; Twitter; and Instagram. The survey was open to the public for 76 days between March and May of 2021, and every Thursday of the week, the survey was reshared on the social media sites to generate a larger sample population. Overall, this achieved a sample size of 83 respondents. As respondents answered questions on topics which they may not have put much thought into prior to completing the survey, this may have hindered their ability to make decent thought-out conclusions in their answers [77, 78], potentially making a catalyst of unreliable data.

Data Analysis Techniques

The quantitative data collected from the online survey were analysed using IBM SPSS. This software was chosen for the quantitative analysis as it has been used for research in social sciences due to the straightforward approach it offers for a range of analyses and the researcher does not need any mathematical expertise to use this software [79, 80]. Additionally, SPSS allowed for comparative investigation between the data sets to be undertaken to analyse whether there were any strong attitudinal relationships [81]. More specifically, *t* tests and ANOVA (Analysis of Variance) tests were carried out using SPSS to determine whether there were any strong relationships between demographics and the topical questions.

The qualitative data collected from the online survey were thematically analysed utilising Microsoft Word. This software was chosen for the qualitative analysis as it enabled the researcher to see all the qualitative data together and go through the process of thematic analysis using the highlight feature to colour codes and themes, and further use the control find feature to search for particular words or phrases [82]. In order to ensure that important data were not missed, the researcher initially became comfortable with the data taking simple notes on opinions which become apparent prior to beginning the coding and thematic categorising stage [82]. Analysis and interpretation of the qualitative results were conducted in tandem to ensure that any final conclusions were reached following in-depth analysis [83, 84].

Ethical Considerations

The British Society of Criminology's Ethics Statement ensures that within any primary research, safety should be practiced, and ethics should be considered [85]. Prior to the survey being shared, a number of ethical considerations had to be considered to ensure that the researcher and participants were not placed at risk, and if so that the mitigation strategies were made available. The main ethical considerations which related directly to this research's research were consent, confidentiality, anonymity, autonomy and

debriefing. Steps were taken to ensure that respondents were aware of their rights as a participant when they agreed to take part in the research.

Online Surveys is fully compliant with the Data Protection Act 2018 [86] and does not record IP addresses to ensure that complete anonymity is maintained. Furthermore, to ensure the data were kept safe and private, only the researcher had access to the raw data which were stored on a password protected account with Online Surveys on a password protected laptop belonging to the researcher. In accordance with the School of Criminology and Criminal Justice Ethics Committee guidelines, the data were stored in the researchers N drive, and after 10 years it will be destroyed. Before the survey could be disseminated, an ethical review was completed by the SCCJ Ethics Committee of the proposed research, and the ethics were approved.

In order to ensure that participants had informed consent and participation was voluntary, an information sheet was included on the first page of the survey. Participants were informed of their rights throughout the survey process and the data collection process and participants were only able to progress to the questions for the survey once they had confirmed they were over the age of 18 and that they consented to everything in the information sheet. A section on debriefing was placed at the end of the survey upon completion which thanked respondents for their participation in the research. Additionally, as the topic of the research was of sensitive nature and could have affected individuals, three helplines and support websites were provided for participants. Finally, the details of the researcher and supervisor were provided in case any respondents had complaints and/or queries regarding the survey.

Results and Discussion

Overview

Overall findings from the literature review highlighted that there is a lack of a widely accepted definition and framework for cyber terrorism in the UK. Findings further discovered that theory can be used to better understand cyber terrorist behaviour, thus aiding in a better understanding of what cyber terrorism is. The literature review, paired with this research's primary data collection, aimed to establish a current definition of cyber terrorism and framework approach which can be utilised by direct stakeholders involved in the prevention, detection, investigation, and prosecution of cyber terrorism within the UK. The research hypotheses were as follows:

1. This research hypothesised that misconceptions may be held amongst the general public, especially in the

qualitative data, and that this could be a representation of misconceptions held amongst direct stakeholders as they are disseminating this information to the general public

2. This research also hypothesised that, based on the demographic characteristics of the sample population, significant effects would be found between the gender demographic and the topical questions where females may have been more concerned with the psychological effects of terrorism and males more so with the physical effects. This hypothesis is influenced by research that has found females to hold greater empathic concerns towards individuals' situations than males [87, 88].
3. In addition, it was hypothesised that significant effects would be found in respondents' occupations, assuming that occupations from within technology and/or law enforcement categories may hold a more experiential understanding of cyber terrorism within the survey.

Quantitative findings are presented through the use of tables, and qualitative findings are explored through themes supported by quotations from the sample population. Subsequently, the results are discussed, exploring interpretations and implications of the findings in light of the learnt literature. This chapter ultimately develops a definition and framework for cyber terrorism informed by available literature presented in the literature review, and the outcomes of the primary data collection.

Demographics of Sample Population

The primary data were collected from 83 respondents overall. Of the sample population, 45% were male respondents and 55% were female respondents. In context of the age demographic, the highest rate of respondents being amongst the '18–24' group and the lowest number of respondents being from the '65 or above' group. As the survey was distributed amongst the researcher's social media accounts, this turnout was expected due to the researcher's connections. The main limitation is the lack of results retrieved from the 65 and above age group, although had this age group been more targeted in the distribution of the survey this would have rejected anonymity and confidentiality of the participants.

The survey offered a total of 25 occupation categories which participants could choose from. Four of these occupations were not selected by any individuals and in addition, some occupations had two or less respondents which implicated the data analysis. Therefore, once all data had been collected, the 21 occupation categories were funnelled down in to nine categories and the data for occupations were recoded in SPSS. The new categories can be seen below in Table 1. The total sample population for occupation is 81 in

Table 1 Sample population according to occupation

Occupation	Total
Business, consulting and finances (A)	10
Student, research and academia (B)	14
Charity work, hospitality and events management (C)	8
Education and public services (D)	11
Engineering, agriculture and construction (E)	7
Healthcare (F)	10
Information technology and media (G)	11
Law enforcement, security and law (H)	6
Transport, retail and tourism (I)	4
Total	81

contrast to the overall population of 83 as two participants did not disclose their occupation.

Quantitative Results

The quantitative results in this primary data collection aimed to investigate whether demographic characteristics from the sample population had any significant effects on the topical questions from the survey. Further to the hypotheses of this primary data collection, the quantitative results further aimed to establish whether there were any trends or patterns

which could be used to better understand what perceptions are held by the public and whether there is a trend leaning towards unanimity or not. A range of *t* tests and ANOVA tests were used to conduct an overall of 66 basic statistical tests using SPSS to initially investigate significant findings in the data. Overall, 97% of the data were found to have no significant effects, indicating only 2 out of 66 tests had a significant effect.

Gender Findings and Interpretations

Independent *t* tests were conducted to investigate whether or not gender played a significant role in the way the topical questions were answered. The overall results for the *t* test can be found in Table 2 where data can be tracked as significant or insignificant in the *p* value column. As can be seen, the results which found gender to have a significant effect were Q9d and Q13. Although significant results are important to note and interpret, it should be acknowledged that these significant findings merely highlight notions which appear worthy of further investigation and replication [89, 90].

The recruitment and mobilisation question asked participants to rank what they felt were ways in which terrorism was being enabled by cyber capabilities from a list of options. Participants were able to choose 3 options with 1 being the most important and 3 being not as important. As

Table 2 Gender-independent *t* test results (*Rank 1 = highest rank, 2 = lowest rank; *Likert 1 = strongly agree, 5 = strongly disagree)

Gender and topical questions	Male		Female		<i>T</i> (40)	<i>P</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>		
Q5—threat level *Likert	2.62	0.861	2.65	0.849	− 0.162	0.872
Q6—online enabling terrorism *Likert	1.81	0.701	1.57	0.779	1.492	0.139
Q8—prime targets	2.89	2.295	2.73	2.330	0.309	0.758
Q9—enabled terrorism *rank						
a) Psychological warfare	2.29	0.488	2.07	0.917	0.699	0.493
b) Propaganda	1.64	0.810	1.65	0.745	− 0.064	0.950
c) Online indoctrination	2.14	0.710	1.80	8.16	1.497	0.141
d) Recruitment and mobilisation	1.57	0.746	2.04	0.676	− 2.233	0.031
e) Data mining	2.14	1.069	1.88	0.806	0.665	0.513
f) Virtual training	2.00	1.414	3.00	0.000	− 1.633	0.178
g) Planning and co-ordination	2.50	0.514	2.50	0.816	0.000	1.000
h) Fund-raising	2.50	0.926	2.20	0.837	0.588	0.568
Q10—Is Q9 terrorism?	1.27	0.608	1.37	0.771	− 0.640	0.524
Q11—dependent terrorism *rank						
a) Cyber breaches of networks	1.96	0.916	1.77	0.770	0.879	0.383
b) Dissemination of malware	2.06	0.725	2.19	0.750	− 0.521	0.606
c) Exfiltration of digital information	2.00	0.816	1.96	0.706	0.168	0.868
d) Financial theft/fraud	1.89	0.737	2.15	0.925	− 1.008	0.319
e) Denial of service attacks	2.13	0.885	1.67	0.816	1.102	0.283
f) Cyber-attacks that trigger physical damage	2.06	0.873	2.23	0.869	0.763	0.539
Q12—is Q11 terrorism?	1.19	0.518	1.26	0.681	0.216	0.599
Q13—Stakeholder understanding important? *Likert	1.89	0.658	1.40	0.580	3.598	0.001

there were more than 3 options for participants to choose from in this question, it cannot be assumed what 3 meant to people – it could have meant ‘least important’ to some or ‘not as important’ to others.

Results showed that male participants ($M = 1.57$, $SD = 0.746$) ranked recruitment and mobilisation higher than females ($M = 2.04$, $SD = 0.676$) and an independent t-test found this pattern to be significant, $t(44) = -2.23$, $p < 0.05$. First, these data suggest that males are more likely to include recruitment and mobilisation as an enabled form of cyber terrorism than females. Second, these data also allude to the notion that males are potentially more concerned with the concept of recruiting and mobilising new terrorists. As no effect size was calculated due to an outdated version of SPSS, these data cannot be generalised to a larger population.

Some assumptions can be made based on the implications of these findings regarding gender perception on recruitment and mobilisation within terrorist activity. Due to terrorist groups use of online capabilities, the ability to recruit and mobilise individuals has increased through a greater ease in disseminating information to followers [14, 91]. This has especially increased during the pandemic where more individuals have felt anxious, disempowered and alone and have found a sense of community and solace in like-minded groups where inciting violence either in a virtual or physical environment, has been more so attractive than possibly before the pandemic [92].

As discussed in this research’s literature review, recruitment is one of the first steps in the process of terrorist group activity [16]. This information, coupled with the male gender effect on ‘recruitment and mobilisation’, could indicate that males are more concerned with terrorist group actions which have a long-term effect such as recruiting individuals, who may play a direct or indirect role in threatening or causing harm to individuals virtually or physically, further down the process of terrorist group activity. This interpretation could be broadened onto a wider scale looking at stakeholders within cyber terrorism where male police officers make up 69% of the police force [93]. For example, if male police officers are more concerned with the long-term effects of cyber terrorism and are more likely to acknowledge recruitment as a first step in terrorist group activity, there may be a greater interest to detect and combat the terrorist activity being enabled by cyber space before the threat of harm to a community or nation increases. Overall, this could indicate there being a greater ambition to deter terrorism from happening through observing recruitment activity online. In light of these findings, there is a potential for hypothesis 2 to be met on the condition that the study be replicated to calculate the generalisability of these findings.

The final question in the survey, asked participants how strongly they agreed that stakeholders’ understanding of the

term cyber terrorism is important in detecting and preventing terrorism in the UK. Zero participants selected the answers ‘disagree’ and ‘strongly disagree’, and only eight participants selected ‘neutral’ which suggests that there is generally overall agreement amongst the sample population that stakeholder understanding is important. However, results showed that female participants ($M = 1.40$, $SD = 0.580$) were more likely to strongly agree with the stakeholder statement than males ($M = 1.89$, $SD = 0.658$), and an independent t-test confirmed a pattern of significance, $t(72.508) = 3.553$, $p \leq 0.05$. These data suggest that females are more likely to acknowledge the influence that stakeholders’ understanding of cyber terrorism can have on the detection and prevention of terrorism. It also highlights that male participants are potentially more inclined to take a more ‘neutral’ standpoint towards the statement. These data challenge one to consider the impact which stakeholders lacking in gender diversity may have on the understanding, and subsequently the detection and prevention of cyber terrorism.

In light of this finding, it is important to consider gender diversity within agencies and stakeholders who are associated in tackling cyber terrorism, including policy makers and law enforcement. Research regarding gender diversity has found that more diverse work environments can result in broader perspectives within decision-making and greater effectiveness in work delivery [94–96]. In addition, one study showed an inclination from female leadership roles in focusing on preventing and resolving matters [97]. As highlighted, the police work force is 69% males [93] and potentially making this environment more gender diverse may mean a greater emphasis for broader perspectives in understanding cyber terrorism to prevent, detect, and investigate terrorism effectively. Furthermore, recent statistics indicated that 34% of the MPs in the House of Commons are female [98]. Although this statistic has been referred to as record high, this nonetheless indicates a disparity in gender diversity within parliament which could be contributing to the difficulties in developing a unanimous definition of cyber terrorism to enable greater prevention strategies against terrorism. Overall, this finding alludes to the necessity for more gender diversity within stakeholders directly involved in detecting and preventing terrorist activity in the UK.

Age and Occupation Findings and Interpretations

ANOVA tests were carried out to establish whether or not age and occupation played a significant role in determining respondent answers. The overall results for age can be found in Table 3, and the overall results for occupation can be found in Table 4. Where the M or SD display ‘n/a’, this is indicative of results where respondents from a specific category did not respond to a specific question. This is most probably due to the rank questions only allowing

Table 3 Age ANOVA multivariate results (*Rank 1 = highest rank, 2 = lowest rank; *Likert 1 = strongly agree, 5 = strongly disagree)

Age and topical questions	18–24		25–34		35–44		45–54		55–64		65+		F	P	η^2
	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD			
Q5—Threat level *Likert	3.00	0.976	2.77	0.832	2.18	0.809	2.65	0.702	2.45	0.688	2.67	0.577	2.101	0.74	0.120
Q6—Online enabling terrorism *Likert	1.86	0.710	1.69	1.032	1.47	0.514	1.65	0.702	1.73	0.905	1.33	0.577	0.657	0.657	0.041
Q8—prime targets	2.55	2.176	3.08	2.691	2.82	1.912	2.81	2.738	3.27	2.453	1.67	1.155	0.316	0.902	0.020
Q9—enabled terrorism *rank															
a) Psychological warfare	2.50	0.548	1.50	0.707	1.75	0.957	2.33	0.816	2.00	1.00	N/A	N/A	0.987	0.443	0.198
b) Propaganda	1.73	0.799	1.75	0.886	1.45	0.688	1.70	0.823	1.80	0.837	1.00	0.000	0.509	0.768	0.054
c) Online Indoctrination	2.00	0.816	1.80	0.837	2.13	0.835	2.00	0.739	1.86	0.900	1.50	0.707	0.268	0.928	0.032
d) Recruitment and mobilisation	1.82	0.751	1.56	0.527	1.89	0.782	1.50	0.837	2.13	0.835	2.33	0.577	1.035	0.410	0.115
e) Data mining	1.83	0.983	1.80	0.837	1.75	0.957	2.75	0.500	1.75	0.957	N/A	N/A	0.996	0.435	0.181
f) Virtual training	2.33	1.155	N/A	N/A	N/A	N/A	3.00	N/A	N/A	N/A	3.00	0.000	0.375	0.716	0.200
g) Planning and co-ordination	2.18	0.874	2.88	0.354	2.44	0.527	2.50	0.707	2.75	0.500	N/A	N/A	1.522	0.222	0.174
h) Fund-raising	3.00		3.00	0.000	2.60	0.894	2.00	1.000	1.50	0.707	N/A	N/A	1.185	0.387	0.372
Q10—Is Q9 terrorism?	1.18	0.588	1.62	0.870	1.53	0.874	1.35	0.702	1.00	0.000	1.00	0.000	1.583	0.175	0.093
Q11—Dependent terrorism *rank															
a) Cyber breaches of networks	1.72	0.895	1.78	0.833	1.92	0.669	2.00	0.943	1.78	0.972	2.33	0.577	0.373	0.865	0.033
b) Dissemination of malware	2.30	0.675	1.25	0.500	2.13	0.835	2.67	5.77	2.13	0.641	2.00		1.799	0.145	0.243
c) Exfiltration of digital information	1.80	0.632	2.11	0.601	2.00	1.000	1.80	0.837	2.50	0.577	1.00		0.988	0.441	0.141
d) Financial theft/fraud	2.25	0.866	2.00	1.000	2.33	1.033	2.08	0.669	1.75	0.886	1.00	0.000	1.090	0.381	0.123
e) Denial of service attacks	2.17	0.983	2.40	0.894	1.50	0.548	2.00	1.155	2.00		N/A	N/A	0.775	0.557	0.154
f) Cyber-attacks that trigger physical damage	2.00	0.816	2.29	0.951	2.11	0.928	1.90	0.876	3.00	0.000	3.00	0.000	1.047	0.406	0.133
Q12—Is Q11 terrorism?	1.18	0.588	1.31	0.630	1.24	0.664	1.29	0.686	1.18	0.603	1.00	0.000	0.195	0.963	0.013
Q13—Stakeholder understanding important? *Likert	1.64	0.727	1.85	0.689	1.65	0.606	1.56	0.629	1.45	0.688	1.33	0.577	0.574	0.720	0.036

Table 4 Occupation ANOVA multivariate results where occupations are identified according to the labels in Table 1 (*Rank 1 = highest rank, 2 = lowest rank; *Likert 1 = strongly agree, 5 = strongly disagree)

Occupation and topical questions	(A)		(B)		(C)		(D)		(E)		(F)		(G)		(H)		(I)		F	P	η^2
	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD			
Q5—Threat level *Likert	2.70	0.823	3.29	1.069	2.13	0.835	2.45	0.934	2.43	0.535	2.70	0.675	2.64	0.674	2.17	0.408	2.50	1.000	1.871	0.078	0.172
Q6—Online enabling terrorism *Likert	2.10	0.994	1.86	0.535	1.25	0.463	1.82	0.982	1.57	0.535	1.40	0.516	1.64	0.674	1.33	0.516	2.00	1.414	1.338	0.239	0.129
Q8—Prime targets	3.44	2.603	2.50	2.345	1.63	1.408	3.36	2.803	2.43	2.149	2.20	1.751	3.27	2.867	4.17	2.401	2.50	1.000	0.872	0.544	0.089
Q9—Enabled terrorism *rank																					
a) Psychological warfare	3.00		2.00	1.000	3.00		1.67	0.577	2.40	0.894	2.50	0.707	2.00		2.00	1.414	2.00	0.000	0.466	0.856	0.253
b) Propaganda	1.17	0.408	1.56	0.726	1.80	0.837	1.67	0.816	1.00		1.57	0.787	1.71	0.951	1.60	0.548	2.33	1.155	0.710	0.681	0.124
c) Online indoctrination	2.00	0.707	2.00	0.756	2.50	1.000	1.75	0.707	2.33	0.577	1.00	0.000	2.14	0.690	2.33	0.577	2.00	1.155	1.406	0.227	0.233
d) Recruitment and mobilisation	2.00	0.894	1.89	0.782	1.60	0.548	2.50	0.837	1.33	0.577	1.86	0.690	1.40	0.548	1.50	0.707	1.50	0.707	1.227	0.312	0.214
e) Data mining	2.67	0.577	2.67	0.577	1.00	0.000	1.75	0.957	2.00	1.000	2.33	0.577	1.00	0.000	2.00	1.414	N/A	N/A	2.010	0.121	0.484
f) Virtual training	3.00		2.00	1.414	3.00		N/A	N/A	3.00		3.00		N/A	N/A	N/A	N/A	N/A	N/A	1.67	0.930	0.400
g) Planning and co-ordination	2.00	0.000	2.17	0.983	2.25	0.500	3.00	0.000	2.00	0.816	3.00	0.000	2.67	0.516	3.00	0.000	2.00		1.792	0.128	0.374
h) Fund-raising	2.33	1.155	3.00	0.000	3.00		3.00		1.00		2.00		2.67	0.577	1.00		N/A	N/A	1.231	0.424	0.633
Q10—Is Q9 terrorism?	1.30	0.675	1.21	0.579	1.25	0.707	1.64	0.924	1.29	0.756	1.20	0.632	1.64	0.924	1.17	0.408	1.00	0.000	0.753	0.644	0.077
Q11—Dependent terrorism *rank																					
a) Cyber breaches of networks	1.71	0.951	1.69	0.855	1.60	0.548	2.25	0.886	2.33	1.155	1.75	0.707	2.00	0.926	1.75	0.957	1.67	1.155	0.511	0.842	0.076
b) Dissemination of malware	2.00	0.707	2.33	0.516	2.50	1.000	1.80	0.837	2.50	0.707	1.00		1.60	0.548	2.50	0.577	2.00		1.241	0.319	0.293
c) Exfiltration of digital information	2.40	0.894	1.50	0.577	1.83	0.753	2.00	0.707	1.00		2.00	0.707	2.00	8.16	2.00		2.50	0.707	0.747	0.650	0.181
d) Financial theft/fraud	1.80	0.837	2.44	0.726	2.00	1.000	1.50	0.837	2.33	1.033	1.80	0.837	2.00	1.000	2.20	0.837	2.00		0.743	0.653	0.149
e) Denial of service attacks	2.00	1.414	2.00	1.155	1.50	0.707	2.00	0.000	0.167	0.577	2.00	1.414	2.25	0.957	1.00		3.00	0.000	0.557	0.795	0.255
f) Cyber-attacks that trigger physical damage	2.33	0.577	2.00	0.894	2.50	1.000	2.50	1.000	1.67	0.516	2.67	0.816	2.75	0.500	1.67	1.155	1.33	0.577	1.608	0.164	0.300
Q12—is Q11 terrorism?	1.20	0.632	1.00	0.000	1.75	1.035	1.45	0.820	1.00	0.000	1.20	0.632	1.09	0.302	1.17	0.408	1.50	1.000	1.504	0.171	0.143
Q13—Stakeholder understanding important? *Likert	1.44	0.527	1.64	0.745	1.75	0.707	1.55	0.688	1.57	0.787	1.50	0.527	1.73	0.647	1.33	0.516	2.00	0.816	0.511	0.844	0.054

three options to be chosen by each participant to rank in questions 9 and 11. In both these tables, the F value column displays that there were no significant findings with age or occupation. The non-significant results were analysed and the implications of these highlighted.

Discussion on Non-significant Results

The reporting of non-significant results has been much debated amongst academics, with various and differing approaches being encouraged [99, 100]. However, it has been strongly posited that non-significant results should not be assumed to represent homogeneity amongst the sample population [101, 102]. This is due to the fact that a non-significant result merely highlights what population parameter is unlikely, rather than what it is likely to be [103].

It can be assumed that the non-significant findings from this primary research were unable to present evidence for all the hypotheses. In order to determine whether a type I or type II error has occurred, replication of the study and re-analysis of the data would need to be carried out to better understand the non-significant results [103].

In the case of a type II error, it is important to discuss potential influential factors apart from gender, age, and occupation which could have influenced the sample population's beliefs towards the survey questions, thus resulting in non-significant results. Most pertinent to this primary research is the impact which media outlets have potentially had in shaping perceptions surrounding cyber terrorism. In a contemporary society, the news has become more easily accessible through news media websites and social media platforms, which has increased the way in which public opinion is shaped due to the news's gatekeeping process [32, 104, 105].

Although news media outlets are beneficial in making the public aware of current events, the implications could potentially be detrimental for stakeholders involved in detecting and preventing cyber terrorism. If public opinion has been shaped to believe that cyber terrorism mainly involves cyber dependent acts such as denial of service attacks, then this may be what the public look out for and subsequently report to the police (recent news examples include [106–108]). This leaves a gap in which cyber enabled acts of terrorism, such as online terrorist propaganda, may not be as reported by the public due to misconceptions. In turn, this potentially impacts the ability for police to prevent terrorist attacks due to online terrorist activity not being as reported. If a unanimous definition of cyber terrorism could be agreed upon, policy-makers and police could share this through news media outlets to enable the public to have a greater understanding of cyber terrorism, in turn encouraging individuals to identify and report both cyber enabled and cyber-dependent terrorism.

Qualitative Results

Analysis of the qualitative data from the online survey revealed important themes which were evident amongst the majority of the sample population. The qualitative analysis aimed to establish a more in depth understanding of what the public's perceptions are towards cyber terrorism. Analysis highlighted that the majority of participants were generally in agreement, with only a small number of participants expressing more opposing views.

Among the 83 participants and across all the topical questions there were a total of 198 qualitative responses. Qualitative responses appeared to decline as the survey progressed, with the highest response rate to a single question being 75 responses and the lowest at 3 responses. This has the potential to lessen the validity and generalisability of all the qualitative responses; however, coupled with the quantitative data and the findings from the literature review, it may contribute in the justification for developing a cyber terrorism definition and framework. Figure 1 displays codes and themes from the qualitative analysis. In the discussion of the qualitative data, responses will be displayed as 'PX' where 'P' indicates 'Participant' and 'X' an identification number.

Victims of Cyber Terrorism

The first theme which emerged from the qualitative analysis of this research's primary data collection was the distinction between the two victims of cyber terrorism. On the one hand, the 'people' victims of cyber terrorism were highlighted with concerns about "vulnerable" and "young" people raised by P1, P2 and P3, and "uninformed users" raised by P4 and P5. These groups were highlighted as victims of being groomed and recruited in to the terrorist group activity process, but also be victims of virtual and physical verbal attacks from cyber terrorists and extremists. On the other hand, there were also concerns highlighted towards the 'system' victims of cyber terrorism where participants included examples such as "data and resources" (P6), "power grids" (P7), and "interfaces" (P8 & P9). One individual (P10) referred to these more physical impacts of cyber terrorism as being "more traditionally what the term [terrorism] is associated with".

The theme of cyber terrorist victims can be one which encourages confusion as there are different types of victims which could be encapsulated under the cyber terrorism umbrella. McGuire and Dowling's [7] cyber enabled and cyber-dependent classification can be used to categorise victims of cyber terrorism which can further aid in developing a more concise classification. 'Human victims' of cyber terrorism can be victims of both cyber enabled and cyber dependent actions, which has been broken down further into 'human victims of cyber dependent terrorism' (for example,

Fig. 1 Thematic analysis codes and themes from qualitative data. This figure displays the themes and codes which came to light throughout the qualitative analysis of the primary data collected.

These themes and codes are reflective of the views and opinions held by the sample population, which are supported further with quotations in the analysis below

data theft) and ‘human victims of cyber-enabled terrorism’ (for example, verbal abuse on a social media platform). Systems who are victims of cyber terrorism can only be victims to cyber-dependent actions and, therefore, have been classed just as ‘system victims’ (for example, Ransomware attacks on national infrastructure for political gain). These classifications contribute to the development of a framework in this research.

However, it became apparent from the qualitative analysis that there is a blurred line between victims and offenders of terrorist activity with P11, P12 and P13 referring to there being an “ease for terrorists to recruit people” and “alter people’s way of thinking”. These qualitative findings are supported by the findings from the literature review highlighting the complexity in sometimes distinguishing between victim and perpetrator as a result of misconceptions from stakeholders affecting news media outlets [30]. Interestingly, although the individuals being recruited and groomed are in fact victims, in some cases they too become the offenders for the very things they were once victims of. This paradoxical concept can be better understood through the story of Shamima Begum who left the UK at the age of 15 after being recruited to join ISIS. Since the age of 19, she has been trying to return to the UK as she claims she did not

expect to go through everything she did, despite her engaging in known terrorist activity [109, 110]. The supreme court recently ruled that they could not allow Begum to return to the UK as this would create a significant national security risk [111].

As highlighted in Jaishankar’s Space Transition Theory [14], the anonymous nature of cyber environments allows individuals to hide their true identities which could enable individuals to transition from victim to perpetrator with more ease, either intentionally or inadvertently, further accentuated by cognitive inhibition effect and dissociative anonymity [50, 51]. Understanding victims of cyber enabled and cyber dependent terrorist activity could also provide a clearer interpretation of motivated terrorist offenders. Overall, this thematic finding highlights disparities amongst respondents regarding cyber terrorist victims which could be due to the absence of an agreed upon definition and framework detailing what qualifies as a cyber terrorist act. Having a unanimous definition would, therefore, make a clearer distinction between victims and offenders of cyber terrorism.

Increase of Terrorist Online Presence

Another theme which emerged from the qualitative analysis was the way in which respondents emphasised how online capabilities have aided in expanding terrorist activity. P14 alluded to the notion that online platforms “help build a sense of community between members, assist in recruitment, and launch attacks”. Additionally, P15 highlighted the ability which terrorists have “to reach a global audience and form groups which reinforce each other”. There were concerns raised specifically regarding the impact which the COVID pandemic has had on terrorist activity. Although some participants highlighted the risk of terrorism as “lower than before due to COVID” (P16), others seemed to emphasise the advantageous aspects of COVID for terrorist activity as there being “more time to plan” (P17), and one participant nodded at cyber terrorism being “underreported” with the “true scale now being unknown but severe” (P18) due to its greater shift online.

It became evident throughout the qualitative data, that much of the sample population appeared to be mostly in agreement that the threat of terrorism posed through online capabilities is apparent. This is supported by the quantitative findings in Q10 and Q12 where $\geq 80\%$ participants were in agreement that the cyber enabled and cyber dependent acts listed were classed as cyber terrorism. These results also support the findings from the literature review which found that terrorist activity is a process by which the smaller and perhaps less impactful activities are seen to have a domino effect on larger terrorist attacks [16]. For example, recruitment was identified by 12 participants throughout the qualitative responses which is a positive finding as it indicates that individuals are aware of its impact in the process of terrorist activity. In addition, this links back to the significant effect found on gender where males were more likely to rank recruitment and mobilisation higher than females in the quantitative results. Controversially to these findings, P19 stated that “terrorism, the act, is an offensive action, just recruitment and fundraising themselves are not terrorist acts” which was an opinion also raised by P20, P21 and P22. These qualitative findings highlight the presence of common misconceptions held by some individuals regarding cyber terrorism, which is supported by the findings from the literature review. The UK law in fact deems ‘Encouragement of Terrorism’ under The Terrorism Act 2006 [28] and ‘Finance and Money Laundering in relation to terrorism acts’ under The Terrorism Act 2000 [56], as common offences. Although it is positive that respondents appeared to mostly agree on cyber enabled and cyber dependent terrorist offences, the minority of people who did not agree could be only a small representation of the wider public.

In light of the aforementioned theme, the misunderstanding around terrorism offences could also be an attributing

factor in causing the general public’s confusion around who is a victim or a perpetrator of cyber terrorism [18, 30]. The public has a responsibility to report observed criminal activity, and if there is not enough awareness of cyber enabled and cyber dependent terrorism offences, this could have detrimental implications on the investigation and prosecution of cyber terrorist activity in the UK in line with the Action Counters Terrorism (ACT) campaign [112]. Understanding these detrimental effects of misconceptions amongst the general public, could suggest an urgent need for cyber terrorism to be unanimously defined incorporating both cyber enabled and cyber dependent aspects. Overall, these findings allude to the potential misconceptions held amongst the public regarding cyber terrorist activity; however, these cannot be generalised without replicating the study with the aim of gathering data from a larger sample population.

Regulation and Stakeholder Understanding

The qualitative analysis further highlighted a theme regarding the regulation of the internet and stakeholders’ involvement in this. The theme of regulation was not introduced to participants within the survey questions, unlike the previous themes, which perhaps highlights the importance of regulatory processes to the survey respondents, in the context of cyber terrorism. P23, in the context of online platforms, stated that these are “too free a space with little to no sense of regulation”, which was a popular opinion with other respondents using words such as moderation, monitor, and regulation on 19 occasions in the qualitative responses. The issue with the lack of regulation on online platforms was further identified by P24 stating “online platforms provide unchecked means of sharing material” and P25 further suggesting the notion of “rumoured safety measures in place”. Interestingly, positive connotations were not associated with regulation in the qualitative responses potentially indicating dissatisfaction regarding the current approaches to regulating online terrorist activity. This dissatisfaction could be a result of ambiguous guidelines on social media and online platform such as those referred to in qualitative responses—“Facebook” (P26 & P27) and “YouTube” (P28, P29, & P30).

YouTube guidelines state that terrorist organisations are not permitted to utilise their services to conduct a range of terrorist activity, for example, “praising or justifying violent acts carried out by a terrorist organisation” [113]. Facebook states that any entities, such as terrorist organisations, who engage in “serious offline harms” will be condemned alongside any content which praises, supports or represents terrorist organisations [114]. Problematically, these online platforms do not define the term ‘terrorism’. This means that when it comes to regulating and removing certain online content, the service providers can decide what is deemed terrorist or not according to their own perceptions. Looking

at the recent conflict between Israel and Palestine, Hamas, a proscribed terrorist organisation [115], fired rockets into Israel from the Gaza strip due to political and religious differences [116, 117]. At the time of these events, there was justification and condoning across online platforms for the violent actions directed at Israel from Hamas despite Hamas' recognition as a terrorist organisation. Furthermore, media platforms such as YouTube and Facebook condemned Israel's actions, and justification for their retaliation was taken down as 'misinformation'. A more recent example is the Plymouth shooting. Jake Davison, who practiced hate speech against women, incited violence and spoke about his 'incel' (involuntary celibate) alignment on YouTube, killed five innocent individuals [118, 119]. Davison had just short of 100 subscribers on his YouTube channel, and these were 100 missed opportunities to detect this terrorist activity prior to his online terrorist behaviour becoming a physical attack.

These unclear guidelines which are used to regulate online terrorist activity are evidently biased and counter-productive, which may be the reason for the dissatisfaction towards regulating cyber terrorism highlighted from some of the survey respondents. Furthermore, with repressed behaviour in physical environments due to the COVID pandemic [2, 14, 53], this may encourage online terrorist activity alongside the lack of collaborative regulation. The implications of this are that direct stakeholders involved in combatting online terrorist activity, including online platform providers and law enforcement, are perhaps not able to do so effectively due to the absence of a unanimously agreed upon definition. Perhaps a collaborative approach could ensure clearer regulatory guidelines and may further enable the future instalment of the draft Online Safety Bill [60] to be more effective.

Q13 from the survey found that 90% of respondents overall agreed that a definition could enable stakeholders to better understand cyber terrorism, in turn aiding in the detection and prevention of terrorist activity. Although this question only received 10 qualitative responses, 'stakeholders' were referred to in qualitative responses from other questions, with direct mentions being made of the police, policy makers, and online platforms. P31 stated that "If you don't consider something a crime or a precursor to a crime, you won't be looking for it" indicating that unless something is defined as a crime, it will not be identified and reported as such. Furthermore, P32 claimed that there is a need for stakeholders to "understand the objectives of the terrorist and the means used to execute their plans". As discussed in the literature review, pre-cursor crimes could include recruitment, training, or disseminating propaganda which are initial phases in the terrorist activity process [16]. Therefore, P31 and P32 could be implying that these pre-cursor terms are not clearly defined under cyber terrorism which perhaps indicates an absence of these activities not being policed effectively due

to a lack of understanding of terrorist motivations. However, much of the regulation of the internet is controlled by the service providers, and therefore, a more collaborative approach from various stakeholders would perhaps be the most effective way to combat online terrorist activity. This collaborative approach would also ensure that public users of online platforms are safer and more aware of what they can report as terrorist activity, in turn countering future threats posed by terrorism.

Defining Cyber Terrorism

The survey asked participants to expand on how they would define cyber terrorism, and this question received the highest rate of responses from 75 participants. Some respondents classified cyber terrorism into binary models such as "hard and soft" (P33) and "enabled and dependent" (P34). Interestingly, of the 75 responses received for this question, only 40% incorporated terrorism that is both enabled by and dependent on cyber capabilities in their proposed definitions. The remaining 60% of respondents focussed on either cyber enabled or cyber dependent activity. This highlights the confusion that exists within the general public and could be reflective of the general misconceptions which exist, emphasising the need for a unanimous definition of cyber terrorism.

Respondents mostly used the 'cyber' prefix within their definitions, with fewer using terms such as 'online', 'technology', 'internet' and 'virtual'. For example, P35 defined cyber terrorism as "terrorism that uses the cyber domain as a space to carry out its actions", and P36 stated "cyber terrorism is when terrorist organisations enter cyber space and instrumentalise the internet to carry out violence". However, P37 highlighted it as the "use of electronic interventions or resources to disrupt online systems or operations". Despite Gordon and Ford's [44] belief that the cyber prefix is not an effective term, the qualitative results find that this is a term which the respondents appear to be familiar with, which could be reflective of the general public's views. Therefore, attempting to change the cyber prefix to something else, such as Computer Network Operations or Information Warfare [38], could potentially cause further confusion. These findings, coupled with the literature review, imply that a cyber terrorism definition could encapsulate a classification between enabled and dependent activity. The implications of a clearer definition, as discussed above in the aforementioned themes, would enable stakeholders including law enforcement, online platform providers, policy makers, and prosecution services to work collaboratively towards a unified goal. This may further enhance the public's understanding of what they could be identifying and reporting in line with the ACT campaign [112].

Establishing a New Approach Towards Cyber Terrorism

In the context of the findings from the literature review and the collected primary data, this research posits a new definition and framework of cyber terrorism which could be utilised by stakeholders directly involved in preventing, detecting, investigating and prosecuting cyber terrorism.

Cyber Terrorism Definition

The development of a cyber terrorism definition aimed to gather the strengths of previously discussed definitions and incorporate them in a clear and more concise manner that can be easily understood. The most important factor which was considered for a cyber terrorism definition to be used by UK stakeholders, was the need for it to be compatible with the definition of Terrorism outlined in The Terrorism Act 2000 [56], The Terrorism Act 2006 [28], The Counter-Terrorism Act 2008 [29], and The Counter-Terrorism and Border Security Act 2019 [57]. In addition, themes from the Foltz [42], Holt [43], and Plotnek and Slay [45] definitions have been considered and prioritised for incorporation in this research's proposed definition. Referring back to the literature review, terrorism as a concept evolves with the times, and henceforth, a cyber terrorism definition should be versatile to ensure its applicability to unpredictable future developments within terrorist techniques. Having identified the most critical components to develop a definition that is both concise and compatible with the legal definition of terrorism in the UK, (binary 'means' classification, motive, intent, and target) the following definition is proposed:

"Cyber terrorism encapsulates cyber enabled activity which intends to advance political, social, or religious ideologies against the public, and cyber dependent activity which further intends to threaten or facilitate damage against the public, properties, and/or systems. Cyber terrorism has the potential to coincide with traditional terrorism".

As identified throughout this research, a clear definition of cyber terrorism could enable a more collaborative approach amongst stakeholders in preventing, detecting, investigating, and prosecuting cyber terrorism. Although this definition is not as lengthy and detailed as some of the other definitions analysed [41, 43, 45], the findings highlighted that a simpler definition with fewer clauses provides greater clarity, encouraging a more unanimous approach across various stakeholders. Overall, by having a clear definition outlined for those involved in detecting and preventing cyber terrorism, this could improve the way in which stakeholders combat the overall threat of terrorism, subsequently enabling the media to relay more accurate information to the public

regarding cyber terrorist activity. This could in turn make the public more confident in identifying and reporting terrorist and cyber terrorist activity in line with ACT [112].

Cyber Terrorism Framework

The development of a framework for cyber terrorism aimed to clearly highlight what kind of terrorist activity occurs in cyber space, the process, and the links between traditional and cyber terrorism. Using the Smith et al. [16] categorisation of traditional terrorist activity, this research proposes a similar approach by incorporating McGuire and Dowling's [7] cyber enabled and cyber dependent dual binary model. As this model has already been adopted by the Crown Prosecution Service to classify and prosecute cybercrimes, it is perhaps important that the same binary model be used to classify cyber terrorism for collaborative work amongst law enforcement and prosecuting services.

Based on this research's proposed definition, a ternary approach is suggested as this highlights the inextricable links between traditional, cyber enabled and cyber dependent terrorism. A proposed ternary model can be seen in the Terrorist Activity Framework in Fig. 2.

This cyber terrorism framework highlights the similarities across the three identified types of terrorism and further accentuates how each of them link into one another with the use of arrows. The different pathways all lead to examples of 'terrorist acts', however, it is important to acknowledge that the first three stages leading up to the fourth stage all have the potential to be occurring simultaneously. In addition, the first three stages in the cyber-enabled pathway have the opportunity to branch out to the fourth stage in the traditional and cyber dependent pathways as much of cyber-enabled activity can be supporting activity for the other pathways. It is further important to highlight that the 'recruitment' stage in traditional terrorism and cyber-enabled terrorism has the ability to remain active throughout the whole process as these activities are not specific to a single terrorist attack. Therefore, stakeholders should consider these ongoing background processes when detecting traditional terrorism and cyber terrorism. Although this framework is limited as it does not list every single type of terrorist offence under each pathway, it nonetheless highlights a few examples which can better inform law enforcement of the intricate relations between each pathway to improve investigative practices in countering terrorism.

Recommendations and Conclusion

This paper, and the research within, intended to contribute to current academic and professional discussion regarding cyber terrorism and how it is defined and understood

Fig. 2 Terrorist activity framework entailing cyber terrorism—developed from [7, 16]. This figure displays a framework which highlights cyber terrorist activity's life cycle. It highlights cyber enabled terrorist activity, cyber-dependent terrorist activity and traditional terror-

ist activity with arrows to show the links between these three components. This framework is put forward from this paper's findings to better aid stakeholders in more collaboratively tackling terrorism

amongst UK stakeholders involved in preventing, detecting, investigating and prosecuting cyber terrorism. Through critically analysing currently established definitions, theories and frameworks related to cyber terrorism, this research highlighted the problematic nature in the lack of a unanimous understanding. In light of this, a new cyber terrorism definition was proposed which incorporates cyber enabled and cyber dependant activity. Furthermore, by developing Smith et al.'s [16] terrorist activity process, this research proposed a potential ternary framework which could be utilised by UK stakeholders to gain a better understanding of cyber terrorist behaviours and their inextricable links to traditional terrorism. Although the definition and framework concisely define and classify cyber terrorism in light of the findings from the literature review and the primary data collection, further editing from stakeholders would be recommended to ensure complete compatibility with UK legislation, and stakeholder procedures. Subsequently, this research recommends that specific legislation regarding cyber terrorism be developed to support UK stakeholders in preventing, detecting, investigating and prosecuting cyber terrorist activity.

Furthermore, although this paper specifically analysed the necessity for a definition and framework in context of the United Kingdom, this proposed definition and framework are nonetheless generic and could, therefore, potentially be adopted for use by other nations. In doing so, a more collaborative international approach could be established to increase the efficacy of countering cyber terrorist activity, overall better securing society from the risk of terrorism.

The secondary aim of this research was to determine what the public's perception of cyber terrorism was through a mixed methods primary data collection approach. The quantitative data highlighted a gender effect on questions regarding recruitment as a cyber-enabled terrorist act, and stakeholder understanding in the context of combatting cyber terrorism. However, the rest of the quantitative data were non-significant and as a result of this, there was not sufficient evidence to substantiate some of the hypotheses surrounding demographic effect on topical questions. In light of the non-significant data, this research further recommends that the primary research be replicated and shared out to a wider audience to generate a larger sample population and

determine whether the non-significant results from the primary data collection are due to type I or type II errors [90, 103]. By gathering a clearer and more generalised understanding of the public's views, UK stakeholders can better identify what the general public's perception is, which could better inform clearer campaigns to educate the public on identifying and reporting cyber terrorist activity.

The literature review highlighted that news media outlets can have an effect on the way in which the public understand a matter, and analysis of the non-significant findings suggested that in the case of a type II error, this could be due to news media outlets' gatekeeping role in disseminating information regarding cyber terrorism to the public [32, 104]. Therefore, this research recommends that further research be carried out regarding the correlation between news media outlets which individuals read/listen to, and their perceptions of traditional and cyber terrorism.

Overall, this research has offered an insight into how cyber terrorism could be defined and classified for UK stakeholders as part of the search for the 'holy grail' [1]. This research specifically highlighted the importance of correlating a new definition and framework with UK legislation for

enhanced compatibility and effectiveness. In current times with the COVID pandemic enabling the evolution of terrorist activity [2], it is ever more important to clearly understand and adapt stakeholder procedures in countering cyber terrorism in the UK.

Appendix A

Survey Questions

The Transition of Terrorism into Cyberspace

Page 1: Welcome to the survey

Hi, I'm Victoria and I am undertaking a Masters in Cybercrime and Intelligence. I am a student in the Institute of Criminal Justice Studies at the University of Portsmouth (UoP). This research contributes to my degree and the results will be used in my thesis. The study is being supervised by the UoP. The findings will assist my research in better understanding what perceptions are held by the public regarding cyberterrorism. You will be asked questions in relation to terrorism and cyberterrorism, but no questions are right or wrong, this is all about your perception. The research complies with data protection regulations (GDPR). Your responses will be entirely anonymous: we will not collect any information that can identify you. The collected data will be securely stored by the UoP for 10 years and then destroyed.

The survey should take around 10-15 minutes to complete. Participation is entirely voluntary. You do not have to answer questions. You can withdraw at any point by navigating away from the web page. However, you cannot modify your answers or withdraw once you have submitted your responses because your participation is anonymous. This online survey is only open for anyone above the age of 18. The topics being covered in this survey (terrorism, cyberterrorism, terrorist activity) may be sensitive to some people, so please take this in to consideration in making an informed decision to take part or not.

If you need more information, please contact me, Victoria Correia, by emailing me at upp846700@myport.ac.uk. You can also contact my supervisor, Iain Reid, at iain.reid@port.ac.uk. The study has been reviewed and approved by the ICJS Ethics Committee. If you have any problems with the study please contact the researcher or supervisor above. If you wish to make a formal complaint, please contact the University at complaints@port.ac.uk.

Institute of Criminal Justice Studies, University of Portsmouth, St George's Building,
141 High Street, Portsmouth PO1 2HY T: 023 9284 8484

By clicking the consent button below, you agree to take part in the study as described above and that you are aged 18 or over.

1. Please indicate your consent to participating in this survey. ☐ Required

☐ I consent

Page 2: Demographics

2. Please indicate your gender

- ☐ Male
- ☐ Female
- ☐ Other
- ☐ Prefer not to say

3. Please select the category which includes your age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64

4. What sector does your occupation fit in to from the list below?

☐ Accountancy, banking and finance	☐ Business, consulting and management	☐ Charity and voluntary work
☐ Creative arts and design	☐ Education and teaching	☐ Energy and utilities
☐ Engineering and manufacturing	☐ Environment and agriculture	☐ Healthcare
☐ Hospitality and events management	☐ Information Technology	☐ Law
☐ Law enforcement and security	☐ Leisure, sport and tourism	☐ Marketing, advertising and PR
☐ Media and internet	☐ Property and construction	☐ Public services and administration
☐ Recruitment and HR	☐ Research and academia	☐ Retail and sales
☐ Science and pharmaceuticals	☐ Social care	☐ Student
☐ Transport and logistics		
☐		

Page 3: Topical questions

5. In your opinion, what threat level does terrorism currently impose on the UK?

	Extremely severe	Severe	Moderate	Slightly	Not at all
Rank opinion	☐	☐	☐	☐	☐

Please don't select more than 1 answer(s) per row.

- 5.a. Please feel free to expand on your answer in more detail in the free text space provided.

6. How far do you agree that online platforms are enabling terrorism?

Please don't select more than 1 answer(s) per row.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Rank opinion	☐	☐	☐	☐	☐

- 6.a. Please feel free to expand on your answer in more detail in the free text space provided.

7. How would you define the term 'cyberterrorism'?

8. In your opinion, who is the prime target for terrorists using online platforms?

- ☐ Current and potential future supporters of the terrorist group The targeted direct victims
- ☐ Potential sympathetic sectors of domestic and foreign audiences Neutral distant audiences
- ☐ Rivalry terrorist groups (e.g. showing more prominence)
- ☐ Adversary/ies of the terrorist organisation (people terrorists are fighting against) The media
- ☐ Other
- ☐
- ☐
- ☐

8.a. If you selected Other, please specify:

8.b. Please feel free to expand on your answer in more detail in the free text space provided.

9. In which ways do you believe terrorism is enabled by a cyber/online environment? Please rank your answers, 1 being the way in which it is most used.

Please don't select more than 1

answer(s) per row. Please select exactly

3 answer(s).

Please don't select more than 1 answer(s) in any single column.

	1	2	3
Psychological warfare	☐	☐	☐
Propaganda	☐	☐	☐
Online indoctrination	☐	☐	☐
Recruitment and mobilisation	☐	☐	☐
Data mining (analysing data on a large scale to generate new information)	☐	☐	☐
Virtual training	☐	☐	☐
Planning and co-ordination	☐	☐	☐
Fund-raising	☐	☐	☐
Other	☐	☐	☐

- 9.a. If you selected Other, please specify:

- 9.b. Please feel free to expand on your answer in more detail in the free text space provided.

10. Do you believe that the acts described above in Q9 qualify as examples of 'cyberterrorism'?

- ☐ Yes
☐ No
☐ Not sure

- 10.a. Please feel free to expand on your answer in more detail in the free text space provided.

11. In which ways do you believe terrorism is dependent on a cyber/online environment?

Please rank your answers, 1 being the way in which it is most used.

Please don't select more than 1
answer(s) per row. Please select exactly
3 answer(s).

Please don't select more than 1 answer(s) in any single column.

	1	2	3
Cyber breaches of networks	☐	☐	☐
Dissemination of malware	☐	☐	☐
Exfiltration of digital information	☐	☐	☐
Financial theft/fraud	☐	☐	☐
Denial of service attacks	☐	☐	☐
Cyber attacks that trigger physical damage	☐	☐	☐
Other	☐	☐	☐

11.a. If you selected Other, please specify:

11.b. Please feel free to expand on your answer in more detail in the
free text space provided.

12. Do you believe that the acts described above in Q11 qualify as examples of
'cyberterrorism'?

- ☐ Yes
☐ No
☐ Not sure

12.a. Please feel free to expand on your answer in more detail in the free text space provided.

13. How strongly do you agree that stakeholders' understanding of the term cyberterrorism could aid the detection and prevention of terrorism in the UK? (Stakeholders include those directly involved in dealing with cyber terrorism for example - law enforcement, policy makers, etc).

Please don't select more than 1 answer(s) per row.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Rank opinion	☐	☐	☐	☐	☐

13.a. Please feel free to expand on your answer in more detail in the free text space provided.

Funding Not applicable.

Availability of Data and Material Raw data not available.

Code Availability Not applicable.

Declarations

Conflict of interest The corresponding author states that there are no conflicts of interest.

Ethical Approval Favourable ethical opinion granted by the School of Criminology and Criminal Justice Ethics Committee from the University of Portsmouth on 05/03/2021.

Consent to Participate Not applicable.

Consent for Publication Not applicable.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Perry NJ. The numerous federal legal definitions of terrorism: the problem of too many grails. J Legis. 2004;30(2):249–74.
2. Tony Blair Institute for Global Change. Snapshot: how extremist groups are responding to COVID-19. Tony Blair Institute for

- Global Change. 2020. <https://institute.global/sites/default/files/2020-05/Snapshot%20%20COVID19%20V02.pdf>
3. Bieda D, Halawi L. Cyberspace: a venue for terrorism. *Issues Inf Syst.* 2015;16(3):33–42.
4. Arora B. Exploring and analysing Internet crimes and their behaviours. *Perspect Sci.* 2016;8:540–2. <https://doi.org/10.1016/j.pisc.2016.06.014>.
5. Marsili M. The war on cyberterrorism. *Democr Secur.* 2018;15(2):172–99. <https://doi.org/10.1080/17419166.2018.1496826>.
6. Luijckx E. Definitions of cyber terrorism. In: Staniforth A, Bosco F, editors. *Cyber crime and cyber terrorism investigator's handbook*. Amsterdam: Elsevier Science; 2014. p. 11–7.
7. McGuire M, Dowling S. Cybercrime: a review of the evidence: summary of key findings and implications. Home Office Research Report 75. London: Home Office, October. 2013. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
8. Home Office. Operation of police powers under the Terrorism Act 2000 and subsequent legislation: arrests, outcomes and stop and search Great Britain, financial year ending March 2020. Home Office National Statistics. 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/891341/police-powers-terrorism-mar2020-hosb1520.pdf
9. Home Office. Operation of police powers under the Terrorism Act 2000 and subsequent legislation: arrests, outcomes, and stop and search Great Britain, year ending March 2021. 2021. <https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-financial-year-ending-march-2021/operation-of-police-powers-under-the-terrorism-act-2000-and-subsequent-legislation-arrests-outcomes-and-stop-and-search-great-britain-year-ending#arrests-and-outcomes>
10. Kshetri N. The global cybercrime industry. Berlin: Springer; 2010.
11. Bernat F, Makin D. Cybercrime theory and discerning if there as a crime: the case of digital piracy. *Int Rev Mod Sociol.* 2014;40(2):99–119.
12. Yunos Z, Sulaman S. Understanding cyber terrorism from motivational perspectives. *J Inf Warf.* 2017;16(4):1–13.
13. Helbing D, Brockmann D, Chadefaux T, Donnay K, Blanke U, Woolley-Meza O, Moussaid M, Johansson A, Krause J, Schutte S, Perc M. Saving human lives: what complexity science and information systems can contribute. *J Stat Phys.* 2014;158:735–81. <https://doi.org/10.1007/s10955-014-1024-9>.
14. Jaishankar K. Establishing a theory of cyber crimes. *Int J Cyber Criminol.* 2007;1(2):7–9. <https://doi.org/10.5281/ZENODO.18792>.
15. Cohen LE, Felson M. Social change and crime rate trends: a routine activity approach. *Am Sociol Rev.* 1979;44(4):588–608. <https://doi.org/10.2307/2094589>.
16. Smith BL, Cothren J, Roberts P, Damphousse KR. Geospatial analysis of terrorist activities: the identification of spatial and temporal patterns of preparatory behaviour of international and environmental terrorists. *Terror Res Center Fulbright Coll.* 2008;222909:14.
17. Enders W, Sandler T. The political economy of terrorism. 2nd ed. Cambridge: Cambridge University Press; 2012.
18. Hoffman B. Inside terrorism. 3rd ed. New York: Colombia University Press; 2017.
19. Sandler T. Terrorism and counterterrorism: an overview. *Oxf Econ Pap.* 2015;67(1):1–20. <https://doi.org/10.1093/oxep/gpu039>.
20. Anderson D. Shielding the compass: how to fight terrorism without defeating the law. *SSRN Electron J.* 2013. <https://doi.org/10.2139/ssrn.2292950>.
21. Greene A. Defining terrorism: one size fits all? *Int Comp Law Q.* 2017;66(2):411–40. <https://doi.org/10.1017/S0020589317000070>.
22. Hewer CJ, Taylor W. Deconstructing terrorism: Politics, language and social representation. In: Roberts R, editor. *Just war: psychology and terrorism*. London: PCCS Books; 2007. p. 199–212.
23. Monroe KR, Kreidie LH. The perspective of Islamic fundamentalists and the limits of rational choice theory. *Polit Psychol.* 2002;18(1):19–43. <https://doi.org/10.1111/0162-895X.00043>.
24. Lee RD. Religion and politics in the Middle East. 2nd ed. New York: Routledge; 2013.
25. Fox J. Separation of religion and state and secularisation in theory and in practice. *Relig State Soc.* 2011;39(4):384–401. <https://doi.org/10.1080/09637494.2011.621675>.
26. Nikfar J. Globalisation and future of power relations in the Arabic Middle-East: a case study of Egypt and Libya. *Humanit Soc Sci Commun.* 2020;7:134. <https://doi.org/10.1057/s41599-020-00631-7>.
27. Stocchetti M. The politics of fear: A critical inquiry into the role of violence in 21st century politics. In: Hodges A, Nilep C, editors. *Discourse, war and terrorism*. Amsterdam: John Benjamin's Publishing Company; 2007. p. 223–48.
28. Terrorism Act 2006, c.11. 2006. <https://www.legislation.gov.uk/ukpga/2006/11/contents>
29. Counter-Terrorism Act 2008, c.28. 2008. <https://www.legislation.gov.uk/ukpga/2008/28/contents>
30. Fine J. Political and philological origins of the term 'terrorism' from the ancient near east to our times. *Middle East Stud.* 2010;46(2):271–88.
31. Lewin K. Frontiers in group dynamics: II. Channels of group life; social planning and action research. *Hum Relat.* 1947;1(2):143–53. <https://doi.org/10.1177/001872674700100201>.
32. Shoemaker PJ, Vos T. Gatekeeping theory. 1st ed. Amsterdam: Routledge; 2009.
33. White DM. The "Gate Keeper": a case study in the selection of news. *Journal Mass Commun Q.* 1950;27(4):383–90. <https://doi.org/10.1177/107769905002700403>.
34. Tabansky L. Basic concepts in cyber warfare. *Mil Strateg Aff.* 2011;3(1):75–92.
35. Weiner N. Cybernetics or control and communication in the animal and the machine. London: MIT Press; 1948.
36. Gibson W. *Neuromancer*. London: Orion Publishing Co.; 1948.
37. Collin J, Flutter A. Reassessing the revolution in military affairs: transformation evolution and lessons learnt. London: Palgrave; 2015.
38. Flutter A. 'Cyber' semantics: why we should retire the latest buzzword in security studies. *J Cyber Policy.* 2018;3(2):201–16. <https://doi.org/10.1080/23738871.2018.1514417>.
39. Lehto M, Huhtinen A, Jantunen S. The open definition of cyber: technology or a social construction? *Int J Cyber Warf Terror.* 2011;1(2):1–9. <https://doi.org/10.4018/ijcwt.2011040101>.
40. Conway M. Reality check: assessing the (un)likelihood of cyberterrorism. In: Chen TM, Jarvis L, Macdonald S, editors. *Cyberterrorism: understanding, assessment, and response*. Berlin: Springer; 2014. p. 103–21.
41. Denning DE. A view of cyberterrorism 5 years later. In: Himma KE, editor. *Internet security: hacking, counterhacking, and society*. Burlington: Jones and Bartlett Publishers; 2006. p. 123–39.
42. Foltz BC. Cyberterrorism, computer crime, and reality. *Inf Manag Comput Secur.* 2004;12(2):154–66. <https://doi.org/10.1108/09685220410530799>.
43. Holt TJ. Exploring the intersections of technology, crime, and terror. *Terror Polit Violence.* 2012;24(2):337–54. <https://doi.org/10.1080/09546553.2011.648350>.

44. Gordon S, Ford R. Cyberterrorism? *Comput Secur.* 2002;21(7):636–47. [https://doi.org/10.1016/S0167-4048\(02\)01116-1](https://doi.org/10.1016/S0167-4048(02)01116-1).
45. Plotnek JJ, Slay J. Cyber terrorism: a homogenized taxonomy and definition. *Comput Secur.* 2021;102:1–9. <https://doi.org/10.1016/j.cose.2020.102145>.
46. Choi KS, Lee CS. The present and future of cybercrime, cyberterrorism, and cybersecurity. *Int J Cybersecur Intell Cybercrime.* 2018;1(1):1–4.
47. Choi KS. Computer crime victimisation and integrated theory: an empirical assessment. *Int J Cyber Criminol.* 2008;2(1):308–33.
48. McQuade SC. Understanding and managing cybercrime. London: Pearson; 2006.
49. Choi KS, Scott TM, LeClair DP. Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *Int J Forensic Sci Pathol.* 2016;4(7):253–8. <https://doi.org/10.19070/2332-287X-1600061>.
50. Suler J. The online disinhibition effect. *Cyber Psychol Behav.* 2004;7(3):321–6. <https://doi.org/10.1089/1094931041291295>.
51. Agustina JR. Understanding cyber victimization: digital architectures and the disinhibition effect. *Int J Cyber Criminol.* 2015;9(1):35–54. <https://doi.org/10.5281/zenodo.22239>.
52. Lee CS, Choi KS, Shandler R, Kayser C. Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. *J Contemp Crim Justice.* 2021;37(3):333–55. <https://doi.org/10.1177/10439862211001606>.
53. Stalans LJ, Finn MA. Understanding how the internet facilitates crime and deviance. *Vict Offenders.* 2016;11(4):501–8. <https://doi.org/10.1080/15564886.2016.1211404>.
54. Crown Prosecution Service. Terrorism. 2021. <https://www.cps.gov.uk/crime-info/terrorism>
55. Wilkinson P. Terrorism. In: Gill M, editor. *The handbook of security.* London: Palgrave; 2006.
56. Terrorism Act 2000, c.11. 2000. <https://www.legislation.gov.uk/ukpga/2000/11/contents>
57. Counter-Terrorism and Border Security Act 2019, c.3. 2019. <https://www.legislation.gov.uk/ukpga/2019/3/contents/enacted>
58. Bertram L. Terrorism, the internet and the social media advantage: Exploring how terrorist organisations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism. *J Deradicalisation.* 2016;7:225–52.
59. Holt TJ. Regulating cybercrime through law enforcement and industry mechanisms. *Ann Am Acad Polit Soc Sci.* 2018;679(1):140–57. <https://doi.org/10.1177/0002716218783679>.
60. Department for Digital, Culture, Media and Sport. Draft Online Safety Bill (CP405). London. 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf
61. Wingfield R. First thoughts on the UK's Draft Online Safety Bill. Global Partners Digital. 2021. <https://www.gp-digital.org/first-thoughts-on-the-uks-draft-online-safety-bill/>
62. Woods L, Perrin W. The Draft Online Safety Bill: Carnegie UK Trust initial analysis. Carnegie UK Trust. 2021. <https://www.carnegieuktrust.org.uk/blog/the-draft-online-safety-bill-carnegie-uk-trust-initial-analysis/>
63. Crown Prosecution Service. Cybercrime - Prosecution Guidance. 2019. <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>
64. Archibald MM, Radil AI, Zhang X. Current mixed methods practices in qualitative research: a content analysis of leading journals. *Int J Qual Methods.* 2017;14(2):5–33. <https://doi.org/10.1177/160940691501400205>.
65. Brannen J. Mixing methods the entry of qualitative and quantitative approaches into the research process. *Int J Soc Res Methodol.* 2007;8(3):173–84. <https://doi.org/10.1080/13645570500154642>.
66. Guthrie G. Basic research methods: an entry to social science research. London: SAGE Publications; 2010.
67. Hatch MJ. Organisation theory: modern, symbolic and postmodern perspectives. Oxford: Oxford University Press; 2012.
68. Elmir R, Schmied V, Jackson D, Wilkes L. Interviewing people about potentially sensitive topics. *Nurse Res.* 2011;19(1):12–6. <https://doi.org/10.7748/nr2011.10.19.1.12.c8766>.
69. Evans JR, Mathur A. The value of online surveys. *Internet Res.* 2005;15(2):195–219. <https://doi.org/10.1108/10662240510590360>.
70. Lewis-Beck MS, Bryman A, Liao TF. *The SAGE encyclopedia of social science research methods.* London: SAGE Publications; 2004.
71. Sue VM, Ritter LA. *Conducting online surveys.* London: SAGE Publications; 2012.
72. Jisc Online Surveys. Jisc Online Survey Tool. 2021. <https://www.onlinesurveys.ac.uk/>
73. Etikan I, Musa SA, Alkassim RS. Comparison of convenience sampling and purposive sampling. *Am J Theor Appl Stat.* 2015;5(1):1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>.
74. Jager J, Putnick DL, Bornstein MH. More than just convenient: the scientific merits of homogeneous convenience samples. *Monogr Soc Res Child Dev.* 2017;82(2):13–30. <https://doi.org/10.1111/mono.12296>.
75. Andrade C. The inconvenient truth about convenience and purposive samples. *Indian J Psychol Med.* 2020;43(1):86–8. <https://doi.org/10.1177/0253717620977000>.
76. Balter F, Brunet I. Social research 2.0: virtual snowball sampling method using Facebook. *Internet Res.* 2012;22(1):57–74. <https://doi.org/10.1108/10662241211199960>.
77. Andrade C. The limitations of online surveys. *Indian J Psychol Med.* 2020;42(6):575–6. <https://doi.org/10.1177/0253717620957496>.
78. Brace I. Questionnaire design: how to plan, structure and write survey material for effective market research. 4th ed. London: Kogan Page; 2018.
79. Miller RL, Acton C, Fullerton DA, Maltby J. *SPSS for social scientists.* London: Palgrave Macmillan; 2002.
80. Ozgur C, Kleckner M, Li Y. Selection of statistical software for solving big data problems: a guide for businesses, students and universities. *SAGE Open.* 2015;5(2):1–12. <https://doi.org/10.1177/2158244015584379>.
81. Stehlik-Barry K, Babinec AJ. *Data analysis with IBM SPSS statistics.* Birmingham: Packt Publishing; 2017.
82. Lester JN, Cho Y, Lochmiller CR. Learning to do qualitative data analysis: a starting point. *Hum Resour Dev Rev.* 2020;19(1):94–106. <https://doi.org/10.1177/1534484320903890>.
83. Busetto L, Wick W, Gumbinger C. How to use and assess qualitative research methods. *Neurol Res Pract.* 2020;2(14):1–10. <https://doi.org/10.1186/s42466-020-00059-z>.
84. Fossey E, Harvey C, McDermott F, Davidson L. Understanding and evaluating qualitative research. *Austral N Z J Psychiatry.* 2002;36(6):717–32. <https://doi.org/10.1046/j.1440-1614.2002.01100.x>.
85. British Society of Criminology. Statement of ethics. British Society of Criminology. 2015. <https://www.britisoccrim.org/documents/BSCEthics2015.pdf>
86. Data Protection Act 2018, c.12. 2018. <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
87. Hoffman ML. Sex differences in empathy and related behaviours. *Psychol Bull.* 1977;84(4):712–22. <https://doi.org/10.1037/0033-2909.84.4.712>.
88. Mestre MV, Samper P, Frías MD, Tur AM. Are women more empathetic than men? A longitudinal study in adolescence. *Span*

- J Psychol. 2013;12(1):76–83. <https://doi.org/10.1017/S1138741600001499>.
89. Szucs D, Ioannidis JPA. Empirical assessment of published effect sizes and power in the recent cognitive neuroscience and psychology literature. *PLoS Biol.* 2021;15(3):1–18. <https://doi.org/10.1371/journal.pbio.2000797>.
 90. Goodman S. A dirty dozen: twelve p-value misconceptions. *Semin Hematol.* 2008;45(3):135–40. <https://doi.org/10.1053/j.seminhematol.2008.04.003>.
 91. Speckhard A, Ellenberg MD. ISIS in their own words: recruitment history, motivations for joining, travel, experiences in ISIS, and disillusionment over time – analysis of 220 in-depth interviews of ISIS returnees, defectors and prisoners. *J Strateg Secur.* 2020;13(1):82–127.
 92. Kruglanski AW, Gunaratna R, Ellenberg M, Speckhard A. Terrorism in time of the pandemic: exploiting mayhem. *Glob Secur.* 2020;5(1):121–32. <https://doi.org/10.1080/23779497.2020.1832903>.
 93. Home Office. Police workforce, England and Wales, as at 31 March 2020 second edition. Home Office National Statistics. 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/955182/police-workforce-mar20-hosb2020.pdf
 94. Profeta P. Gender equality in decision-making positions: the efficiency gains. *Intereconomics.* 2017;52:34–7. <https://doi.org/10.1007/s10272-017-0640-4>.
 95. Rose C. Does female board representation influence firm performance? The Danish Evidence. *Corp Gov Int Rev.* 2007;15(2):404–13. <https://doi.org/10.1111/j.1467-8683.2007.00570.x>.
 96. Sarhan AA, Ntim CG, Al-Najjar B. Board diversity, corporate governance, corporate performance and executive pay. *Int J Financ Econ.* 2018;24(2):761–86. <https://doi.org/10.1002/ijfe.1690>.
 97. Van Der Walt N, Ingley C. Board dynamics and the influence of professional background, gender and ethnic diversity of directors. *Corp Gov Int Rev.* 2003;11(3):218–34. <https://doi.org/10.1111/1467-8683.00320>.
 98. Uberoi E, Watson C, Mutebi N, Danechi S, Bolton P. Women in politics and public life (Breifing Paper Number 01250). House of Commons Library. 2021. <https://researchbriefings.files.parliament.uk/documents/SN01250/SN01250.pdf>
 99. Hartgerink CHJ, Wicherts JM, Van Assen MALM. Too good to be false: nonsignificant results revisited. *Collabra.* 2017;3(1):1–18. <https://doi.org/10.1525/collabra.71>.
 100. Visentin DC, Cleary M, Hunt GE. The earnestness of being important: reporting non-significant statistical results. *J Adv Nurs.* 2019;76(4):917–9. <https://doi.org/10.1111/jan.14283>.
 101. Greenland S, Senn SJ, Rothman KJ, Carlin JB, Poole C, Goodman SN, Altman DG. Statistical tests, *P* values, confidence intervals and power: a guide to misinterpretations. *Eur J Epidemiol.* 2016;31:337–50. <https://doi.org/10.1007/s10654-016-0149-3>.
 102. Higgins JPT, Thompson SG, Deeks JJ, Altman DG. Measuring inconsistency in meta-analysis. *BMJ.* 2003;327(557):557–60. <https://doi.org/10.1136/bmj.327.7414.557>.
 103. Aberson C. Interpreting null results: improving presentation and conclusions with confidence intervals. *J Artic Supp Null Hypothesis.* 2002;1(3):36–42.
 104. Vermeer S, Trilling D, Kruijkemeier S, Vreese C. Online news user journeys: the role of social media, news websites, and topics. *Digit J.* 2020;8(9):1114–41. <https://doi.org/10.1080/21670811.2020.1767509>.
 105. Welbers K, Opgenhaffen M. Social media gatekeeping: an analysis of the gatekeeping influence of newspapers' public Facebook pages. *New Media Soc.* 2018;20(12):4728–47. <https://doi.org/10.1177/1461444818784302>.
 106. Boris T. Russian hackers target president Vladimir Putin's Phone-In, Major Telco Confirms cyberattack. *Tech Times.* 2021. <https://www.techtimes.com/articles/262260/20210701/hackers-cyber-attack-russian-president-putin-s-phone-in.htm>
 107. Robinson C. Northern's ticket machines hit by ransomware cyber attack. *BBC News.* 2021. <https://www.bbc.co.uk/news/uk-england-57892711>
 108. Russon M. US fuel pipeline hackers 'didn't mean to create problems'. *BBC News.* 2021. <https://www.bbc.co.uk/news/business-57050690>
 109. BBC News.. Shamima Begum: 'I didn't want to be IS poster girl'. *BBC News.* 2021. <https://www.bbc.co.uk/news/uk-47276572>
 110. Casciani D. Shamima Begum: What can the UK do about the IS teenager?. *BBC News.* 2019. <https://www.bbc.co.uk/news/uk-47240100>
 111. BBC News. Shamima Begum cannot return to UK, Supreme Court rules. *BBC News.* 2021. <https://www.bbc.co.uk/news/uk-56209007>
 112. Home Office. CONTEST the United Kingdom's strategy for countering terrorism. 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3_0_WEB.pdf
 113. YouTube. YouTube Policies Violent Criminal Organisations Policy. YouTube Help. 2021. https://support.google.com/youtu/be/answer/9229472?hl=en&ref_topic=9282436
 114. Facebook. Community standards violence and criminal behaviour. Facebook Community Standards. 2021. https://www.facebook.com/communitystandards/violence_criminal_behavior
 115. Home Office. Proscribed terrorist groups or organisations. Gov UK. 2021. <https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2/proscribed-terrorist-groups-or-organisations-accessible-version>
 116. Holmes O, Beaumont P. Israel launches airstrike on Gaza Strip after Hamas rocket attacks. *The Guardian.* 2021. <https://www.theguardian.com/world/2021/may/10/hamas-fires-rockets-into-israel-in-dispute-over-jerusalem-mosque>
 117. Srivastava M. Hamas rocket attacks provoke Israeli retaliation in Gaza. *Financial Times.* 2021. <https://www.ft.com/content/887f0b34-1e08-428c-92c0-603e7830ba5b>
 118. Bancroft H, Mathers M, Tidman Z. Jake Davison named as Plymouth shooter: what we know so far. *The Independent.* 2021. <https://www.independent.co.uk/news/uk/home-news/jake-davison-on-plymouth-shooting-b1901948.html>
 119. Hardy J, Gardner B, Lyons I. 'I am a terminator' boasted Plymouth gunman Jake Davison in final YouTube video before rampage. *The Telegraph.* 2021. https://www.telegraph.co.uk/news/2021/08/14/plymouth-shooting-gunman-said-terminator-final-youtube-video/?li_source=LI&li_medium=liftigniter-onward-journey

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.