JCMS Journal of Common Market Studies UACES
JCMS 2021 Volume 00. Number 0. pp. 1–20 DOI: 10.1111/jcms.13300

Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis

CHRISTOPHER BAKER-BEALL[1] and GARETH MOTT[2]
[1]Disaster Management Centre, Bournemouth University, Bournemouth [2]Institute of Advanced Studies in Cyber Security and Conflict (SoCyETAL), University of Kent, Canterbury

Abstract

This article analyses the European Union's (EU) construction of the threat of cyberterrorism. Through the application of interpretive discourse analysis, the article identifies several key strands that underpin the construction of the cyberterrorist threat within the political and security institutions of the EU. Locating the analysis within the literature pertaining both to the EU as a security actor and to cyber-security, the article identifies the emergence of the perceived threat of cyberterrorism within the EU discourse on emerging security threats. The article scrutinizes the meaning(s) ascribed to this threat, arguing that although cyberterrorism has not been conclusively defined by the EU, the threat has been invoked as a means of legitimizing existing and future security practices. In particular, the threat of cyberterrorism has been ascribed significance with respect to the need to implement harmonized, high standards for the securing of critical infrastructure across the EU and its member states.

Keywords: Critical Infrastructure; Counter-Terrorism; Cyber-Terrorism; Discourse Analysis; European Union

Introduction: Understanding the European Union as a Coherent Regional Cyber Actor

Reliance upon internet services (*Eurostat*, 2019) entails a greater vulnerability, leading member states of the European Union (EU) to take account of an inverse relationship between prosperity and risk. In alignment with this, the EU has sought to develop its capabilities as a regional cyber-security actor. In February 2013, the EU adopted its first Cyber-Security Strategy with a narrative of countering cybercrime and state-sponsored cyber-attacks. This was followed in April 2015, by the European Agenda on Security, which highlighted coordinated European action in cyber-security as a priority for the EU in the immediate future. These plans for the enhancement of EU policy for cyberspace have been accompanied by enhancements in legislative provisions to tackle cyber threats. In 2013, the EU updated the 2005 directive on Attacks against Information Systems, and in 2019 adopted a new regulation governing the European Cyber-Security Agency (the ENISA) targeted at cybersecurity certification. These measures form part of a broader narrative of EU institutions consolidating a pan-European 'actorness', establishing a 'hub' to help member states standardize and understand risks, including the implementation of measures that may be taken to counteract them. This consolidation includes diffuse threats such as terrorism, and novel threats such as that posed by varying forms of cybercrime.

The EU first began developing a collective counter-terrorism policy in 2001 in the immediate aftermath of the September 11 terrorist attacks in the United States. Initially focusing on the external threat posed by terrorism (European Commission, 2001), the first EU Action Plan on Combatting Terrorism was adopted in November 2001 and was followed later, after the terrorist attacks in Madrid in 2004 and London in 2005, by the EU Counter-Terrorism Strategy (Council of the European Union, 2005b). In the period since, EU counter-terrorism policy has evolved to focus, holistically, on both internal and external security issues that include counter-radicalization, responses to foreign fighters, border security as a counter-terrorism measure and terrorist use of the internet. During this development of EU counter-terrorism policy, the threat from 'cyberterrorism' has been invoked intermittently as a potential future concern for the EU in this area, although with much greater frequency since 2010. At present, there is little research on the EU response to the specific issue of cyberterrorism (see Argomaniz, 2015). This article, therefore, contributes to a small but growing field of literature analysing the EU's role as a regional cyber-security actor, by offering a discourse analysis of how the EU conceptualizes the threat from cyberterrorism.

As such, this article has two main aims. First, to critically analyse the discursive construction of the threat of cyberterrorism within the various bodies of the EU. Second, to assess the relationship between the discursive construction of the threat of cyberterrorism and the formulation of cyber-security policies at EU level. Specifically, this article contributes to the literature on the EU as a holistic security actor (Zwolski, 2012; Baker-Beall, 2016) by analysing the EU response to a threat – cyberterrorism – that has not at the time of writing materialized in any publicly-known instance. It is argued that the threat of cyberterrorism is poorly defined, both within the EU and internationally, and that the EU draws on the threat of cyberterrorism – alongside a broader portfolio of threats – to endorse the necessity of current and future EU security measures and legislative instruments.

I. Literature Review: The EU as an Emerging Cyber-Security and Counter-Terrorism Actor

Academic literature in the field of EU Studies has increasingly sought to explore the EU's emerging role as a cyber-security actor. Christou and Simpson's (2011) analysis of the EU's approach to global governance of the internet stands as an early example of research into the EU's articulation of cyber politics. The EU is placed within the context of a contested field; given the prominence of US-based NGOs in the global governance regime of the internet (for instance, ICANN), the EU must negotiate with other global actors, most notably the USA. In some cases, stated EU aims and objectives have not been met, as EU agents have been rebuffed by their American counterparts (Christou and Simpson, 2011). This narrative, of a regional organization that is proactive in the politics of cyberspace is a common theme through the literature, notwithstanding some critiques (Guitton, 2013; Fahey, 2014; Sliwinski, 2014; Carrapiço and Barrinha, 2017; Christou, 2018).

Sperling and Webber (2019) have argued that the EU can be said to have acted as a 'collective' securitising actor, including in the politics of cyber-security. This collective agency includes the securitisation of 'cyberterrorism and hybrid threats' (European

Commission, 2015; Sperling and Webber, 2019). Likewise, Christou also contends that the EU's collective securitisation of cyberspace is underpinned, like EU responses to terrorism, by three distinct but interrelated EU-level mandates, including 'Freedom, Justice and Security'; the 'Internal Market'; and the 'Common Security and Defence Policy' (Christou, 2019; see also Ruohonen *et al*., 2016). For Renard, the EU's bilateral cyber partnerships with external powers including the USA, Canada, China, India, Russia amongst several others, led to the assertion that the EU could be said 'to perform a "positional" function, in the sense that the Union has managed to assert itself as a worthwhile interlocutor in the cyber domain … embedding them in a network of dialogues, joint statements and common initiatives, in which the EU becomes a hub' (Renard, 2018). Indeed, although issues remain with implementation of policy in this area, it is still the case that the EU can be described as an exceptional regional actor on cyber issues, given that no equivalent organization engages in cyber-security and cyber diplomacy on such a holistic basis (Pawlak, 2019).

At risk of simplification, there are presently two main literatures on EU counter-terrorism policy. The first is a body of research that offers a conventional account of the historical development of policy in this area, which is largely based on historical-institutionalist and public policy making approaches that are situated within the field of European Studies (Kaunert, 2010; Argomaniz, 2011; Bures, 2011; Bossong, 2012). The second body of literature, drawing on interpretive and critical approaches to the study of security, has highlighted the importance of discourse, language and identity (Tsoukala, 2004; Jackson, 2007; Hassan, 2010; Baker-Beall, 2014, 2016), as well as technologies of governance (Bigo, 2007; Wittendorp, 2016a, 2016b), in the creation of security practices and, specifically, the formulation of EU counter-terrorism policy.

In relation to the former, Argomaniz (2011) has offered an institutionalist account of the development of EU counter-terrorism policy, analysing the role of the EU in coordinating member states' policies and highlighting the often complex and multidimensional aspects of the EU's response to the threat from terrorism. Bures (2011) has provided an overview of the array of counter-terrorism measures developed by the EU in the period since 9/11, demonstrating how EU counter-terrorism policy has been beset with problems at member-state level over implementation, leading to questions regarding the effectiveness of the EU as an actor in this specific area. Bossong (2012) has highlighted the importance of terrorist incidents in driving forward EU counter-terrorism policy, noting that the 9/11 attacks created a 'window of opportunity' through which agreement on a whole host of counter-terrorism measures could be agreed. Similarly, Kaunert (2010, p. 11) has noted the important role that supranational 'policy entrepreneurs' such as the European Commission and the Council Secretariat have played, highlighting their 'considerable influence in shaping the current design of the EU counter-terrorism policy'. Furthermore, de Londras and Doody's (2015) edited collection provides an overview of the impact and legitimacy of legislative developments in EU counter-terrorism, and is unique in the sense that it analyses in detail the effectiveness of policy in this area.

Research has also explored EU counter-terrorism policy with a focus on the internal and external security measures that have been agreed amongst the member states. Boin *et al*. (2014) have focused on the internal dimension of the EU response, providing analysis of the institutional capacities of the EU in terms of its approach to 'managing the

terrorist threat'. They highlight several areas of justice and home affairs policy where EU counter-terrorism competencies have increased, including police and judicial cooperation, information exchange, immigration and border control. Eling (2007) has analysed the relationship between the EU and other international intergovernmental actors such as the United Nations, while Rees (2008) investigated the establishment of a bilateral relationship between the EU and the United States in the field of counterterrorism. Likewise, MacKenzie *et al*. (2014) have offered an account of the EU's emerging role as a holistic global counter-terrorism actor.

With regard to the second body of research, a smaller but growing literature has adopted approaches from the field of Critical Security Studies to explore this topic. Baker-Beall (2014, 2016) has offered a discursive analysis of the formulation of EU counter-terrorism policy, noting the important role that the identity of the EU plays in the development of policy in this area. Jackson (2007) has analysed the evolution of the EU's 'fight against terrorism' discourse, which he argues is rooted in a criminal-justice approach to counter-terrorism, which stands in contrast to the exceptional, war-based response favoured by the US. Similarly, Tsoukala (2004) of debates in the European Parliament after the 9/11 attacks, revealed a degree of institutional contestation over perceptions of the terrorist threat and appropriate responses to it. As we discuss below, when analysing debates in the EP where cyberterrorism is invoked, in contrast to Tsoukala's analysis, we highlight a much greater degree of agreement over perceptions of the threat.

Alongside this literature which explores discourse on terrorism at the EU level, there is also a body of research that critically analyses the emergence of security and counter-terrorism practices. Wittendorp (2016a, 2016b), has adopted the Foucauldian concept of 'governmentality' to demonstrate how the EU approach to terrorism can be understood as technologies of governance that bind multiple actors together in the creation of a permanent state of insecurity. Wittendorp's analysis demonstrates similarities with Didier Bigo's argument about the role of vested professionals of the 'management of unease' in the development of EU security policies. Bigo identifies a multiplicity of actors that include domestic and EU politicians, police and intelligence officials, army officers, security experts, journalists and parts of civil society, all of whom simultaneously work together and compete to establish their own political authority in the field of security, with counter-terrorism but one area in this wider field of insecurity. In essence, these transformations in the field of security at the European level reflect what de Goede has termed an emerging 'European security culture'. This culture of security is based around the identification, prevention, anticipation and early intervention in response to security threats that go far beyond just counter-terrorism (de Goede, 2011) which, as we contend below, is also reflected in the EU approach to cyberterrorism.

At the time of writing there has only been one study, Argomaniz's (2015) analysis of 'terrorist use of the internet', that explicitly combines an analysis of cyber-security and counter-terrorism. Argomaniz has highlighted that EU bodies have presented a distorted view of what cyberterrorism is; for example, referring to the use of the internet to commit terrorist offences (such as the dissemination of extremist material) as an example of cyberterrorism (European Parliament, 2011). Argomaniz's analysis has suggested that for the EU, the core concern is the act of a cyber-attack itself, rather than the identity of the perpetrator (2015; see also Council of the European Union, 2010). This line of enquiry is revealing, because in the case of the UK's securitisation of cyberterrorism, the

reverse was found to be true; British securitising actors and vested audiences securitised the identity of purported cyberterrorist actors, rather than the act itself or the malware that would be required to carry out such an attack (Mott, 2019). Securitising the identity of a hypothetical cyberterrorist actor, rather than the act of a generic cyber-attack, meant that British securitising agents were able to leave the discursive construction of the cyber weapons in a neutral space (Mott, 2019).

Notably, although Argomaniz (2015) briefly highlights instances where the EU has referenced the threat of cyberterrorism, the primary focus of his analysis is distinguishing between the development of EU policies to counter the administrative use of the internet by terrorists and other more generic cyber-security policies that have been developed to counter cybercrime. What is currently absent is a study that investigates how the EU has conceptualized the threat from cyberterrorism, including investigation of how the EU's perception of this threat impacts upon its wider cyber-security and counter-terrorism practices. This article is intended to address this gap in the literature. Specifically, this article argues that the EU has projected the threat of cyberterrorism – without defining the threat per se – to legitimize existing and future security policies, as well as EU Directives particularly relating to cyber-security and resilience of critical infrastructure.

II. Interpretive Methodology: Identifying the 'Strands' of European Union Cyberterrorism Discourse

Theoretically, this article is underpinned by previous research on the notion of EU actorness, and particularly the idea that the EU can be understood as an 'intricate' or 'holistic security actor' (see Carrapiço and Barrinha, 2017, pp. 1254; Zwolski, 2012; Baker-Beall, 2016). According to Larsen (2002), the EU can be viewed as demonstrating actorness in that member states have imbued legitimacy on the EU to act on security issues by constructing it as a purposeful actor in international relations. Increasingly, EU responsibilities in the field of security have expanded and now traverse both internal and external security threats, meaning we can speak of the EU as a 'holistic security actor' (see Zwolski, 2012; Baker-Beall, 2016). This expanded remit can be seen in the polices that have been created that concern both cyber-security and (cyber)terrorism. As Carrapiço and Barrinha (2017) explain, the post-Cold War environment brought about this change, with new transnational solutions needing to be devised in order to counter the new and emerging threats posed by terrorists or organized (cyber)criminals. Although we recognize that the EU's aspirations towards becoming a more purposeful actor in the security arena have not always led to more coherence in either counter-terrorism policy (see Bures, 2011) or cyber-security strategy (see Carrapiço and Barrinha, 2017), we contend that the invoking of security threats plays a key role in enhancing moves in this direction.

Therefore, given that the focus of this article is to understand and critique the EU's articulation of the threat of cyberterrorism and its impact on policy, this research applies an interpretive methodology (for instance, see Bevir *et al*., 2013). Moreover, given that terms like terrorism, cyber-security and cyberterrorism are essentially contested concepts, or 'social' rather than objective facts (see Jackson, 2007), we adopt an interpretive discourse analysis approach that enables the discourse to speak for itself. If we are to understand how EU stakeholders 'spoke' cyberterrorism into existence (Conway, 2008), it would

be an error of judgement to project an interpretation onto the agents. This particular study adapts an interpretive approach that has already been deployed by Baker-Beall (2016) in the context of EU counter-terrorism policy and Mott (2019) with respect to the British construction of the threat of cyberterrorism. The authors suggest that novel inferences can be made by adopting this framework and applying it to the discursive construction of the threat of cyberterrorism. This discourse approach draws similarities with the double-reading strategy advocated by Ashley and other scholars of discourse analysis, whereby two readings take place: the first, designed to identify the key themes upon which the discourse rests; and the second, to highlight the relationship between discourse and the practices subsequently enabled (Ashley, 1988).

The first stage in the research process was to identify all of the key texts produced by the EU on the issue of cyberterrorism. Keyword searches for 'cyberterrorism', 'cyberterror', 'cyberterrorist' and variations thereof against the europa.eu website were run across the period from 2001 through to the present day. The year 2001 was selected because it marked the first instance of the term 'cyberterrorism' being used at EU-level discourse. Sources appeared from this first date up to 2020. The authors' manual searches elicited policy documents produced by the European Council and the European Commission, as well as a range of Parliamentary reports and votes, including both oral and written contributions on the issue of cyberterrorism. Each record was then read and screened by the authors to ascertain their applicability to this study of the EU discourse on cyberterrorism. In total there were over 150 documents, including 77 records for the European Council and the European Commission, 150 + records for the European Parliament and 7 Europol TE-SAT reports that directly mentioned the issue of cyberterrorism. Sources were selected if they alluded to cyberterrorism in any language. These sources were selected irrespective of whether they differed in their interpretations of what cyberterrorism was. For instance, although most sources inferred that cyberterrorism would be a serious computer-targeting crime, committed by non-state terrorist group, a small minority of MEPs suggested that states could be culpable of cyberterrorism. Conflicting voices and arguments were consciously collected, mapped and analysed to draw out which narratives alluding to the threat of cyberterrorism were dominant.

Having identified the corpus of texts for analysis, accordingly, the second step in this interpretive approach was to map the discourse, by identifying the components of each source that served to make them function. Each source was scrutinized using three analytical questions. First, in order to ascertain the most prominent terms in the 'cyberterrorism-as-threat' discourse, the authors asked: 'what are the keywords, terms, phrases, labels, metaphors and beliefs in each source?'. Having identified these key words, the authors subsequently asked the question: 'what are the key strands that make up the discourse?'. Here, the term 'strand' is used to label the overarching themes of the discourse, which serve to underpin the threat construction. The final element of the 'mapping' process was implemented to understand how the sources construct the threat of cyberterrorism. In order to do this, the authors asked the question: 'how does the discourse construct the threat of cyberterrorism?'

The third stage of analysis sought to develop a more detailed understanding of the functioning of the discourse. In order to accomplish this, the authors performed a second reading of the sources, applying a further three questions. The authors understand

discourse as performative action, which is gained when there is a partial fixation of meaning; both in terms of the key concepts that underpin the discourse and the threat perception of the actors. Consequently, in order to draw out sites of partial fixation, the authors asked the question: 'how does the discourse partially fix the meaning of cyberterrorism in the EU lexicon'? This was followed by a second question designed to reveal the link between the threat discourse and the interlinked practices legitimized by, or enacted in response to it, namely: 'what knowledge and/or practices does the discourse legitimize, and what knowledge and/or practices does it serve to exclude?'. The sources were then applied against the third and final question, which was: 'to what extent can the construction of the threat of cyberterrorism be considered novel?'. This question sought to identify sites of convergence and divergence in the EU's discourse of cyberterrorism.

It should be noted that although we recognize that the EU consists of a multitude of different agencies that have competing interests and varying competences in the field of security (Jackson, 2007). We also view the EU as a site of discursive authority, with enough consistency across the array of different actors to provide a common institutional language and framework for action in the spheres of cyber-security and counter-terrorism. The authors concur with Balzacq *et al*. (2010), and we premise the ensuing analysis on the view that EU security discourses represent practices that co-mingle as a performance with 'everyday' practices of agents.

Having mapped and analysed the corpus, the authors identified two key strands of the cyberterrorism discourse that remained consistent across all of the EU institutions analysed. First, we demonstrate how the discourse is characterized by a failure to clearly define cyberterrorism, noting that it is not defined in any of the major related security policy documents. However, in the absence of a definition, we highlight several key characteristics that when taken together reflect a common perception or understanding of cyberterrorism as: a hybrid type of terrorist attack, an increasing threat to European society, a threat to democracy, borderless in nature, and a potential future threat that has yet to materialize. The second key strand was the primary referent object to-be-secured: critical infrastructure. The discourse identifying the vulnerability of critical infrastructure to a potential cyberterrorist incident served as a core logic to re-legitimize broader security practices relating to cyber-security and counter-terrorism respectively.

III. The EU Definition of Cyberterrorism

The first recorded instance of the use of the term cyberterrorism by an EU institution was in the Council of the European Union (2002a) action plan for promoting EU–Japan cooperation from January 2002. Cyberterrorism was mentioned as a form of 'cybercrime' and one of a group of potential security threats, which would necessitate increased bilateral cooperation between Europol and Japanese police departments fighting transnational crime. The threat from cyberterrorism was also referenced in the first Terrorism Situation and Trends Report (TE-SAT), released by the Council and Europol, in November 2002 (Council of the European Union, 2002b), as a type of terrorism alongside others such as 'separatist terrorism', 'anarchist terrorist movements', 'bioterrorism', 'left-wing terrorism', 'right-wing terrorism' and 'international terrorism'. Although no cases of cyberterrorism were reported by EU member states it was still referenced in the first four TE-SAT reports, before being dropped until 2012 when reporting of potential

cyberterrorism threats to member states began to appear in the Europol reports with greater frequency.

Interestingly the term cyberterrorism did not appear in the list of terrorist offences outlined in the EU's original Framework Decision on Combating Terrorism (Council of the European Union, 2002c). However, the threat from cyberterrorism was highlighted as a reason for the development of a Framework Decision on Attacks against Information Systems (agreed in 2002), with the EU's proposal for a European-wide Arrest Warrant and the moves to approximate laws on terrorism forming a package of measures that the European Council argued would 'ensure that Member States of the European Union have effective criminal laws in place to tackle cyberterrorism, and will enhance international cooperation against terrorism' (Council of the European Union, 2002c). The Framework Decision on Attacks against Information Systems was signed into law in 2005. However, while it clearly outlined 'the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States' (Council of the European Union, 2005a) as a primary concern necessitating the approximation of relevant criminal law, once again a clear definition of cyberterrorism was missing.

Similarly, the concept of cyberterrorism was also absent from the EU's first Counter-Terrorism Strategy, released in December 2005. At this point, the focus of the EU was on impeding the potential use of the internet by terrorists either to finance attacks, recruit, or 'to communicate and spread technical expertise related to terrorism' (Council of the European Union, 2005b, p. 13). Although overlooked in the original counter-terrorism strategy, the issue of cyberterrorism was identified as one of three main priorities months later in May 2006 as part of the revised EU Action Plan on Combating Terrorism, with a report by the EU CTC noting that a key aspect of international cooperation to combat terrorism should focus on three areas: 'preventing radicalisation and recruitment, combating terrorist financing, and preventing cyberterrorism' (Council of the European Union, 2006).

Concerted effort by the EU to offer a clearer definition of cyberterrorism started in 2010. Following a pattern reminiscent of much of Western counter-terrorism policy, the efforts made by EU policy-makers to define cyberterrorism were largely event-driven. It was the Stuxnet attack in 2010, attributed to the US and directed against Iran, which highlighted the potential vulnerability to attack of the computers systems linked to critical infrastructure in the EU. A discussion paper from the EU Counter-Terrorism Coordinator (CTC), in November 2010, stated clearly that 'the Stuxnet incident in summer has shown again that critical infrastructures can be vulnerable to attacks on their information and communication component' and that while 'cyberterrorism is not the major hazard' (instead highlighting 'criminal networks' and 'state sponsored attacks' as the primary concern), moving forward 'cyber-attacks' should be considered 'attractive for terrorist groups for the same reasons which attract criminal or other hostile actors' and therefore it was important that the EU 'start our preparation before terrorists acquire know-how or capacities to target our infrastructures' (Council of the European Union, 2010).

In July 2011, the EU Working Party on Terrorism (WPT), which leads and manages the European Council's agenda on counter-terrorism issues, began an initiative to collate information on the increasing threat from cyberattacks, with a particular focus on the concept of cyberterrorism. As part of this process, the WPT noted the need for a clearer definition of this concept and proposed that the EU develop 'a glossary of the most important

terms … [which] could possibly result in the identification of the need for legislative changes' (Council of the European Union, 2011b). Indeed, the WPT highlighted not only that 'the concept of cyberterrorism is not yet clearly defined in the EU and there is a need to develop a common understanding of the threat', it would also be necessary to develop 'a clear definition of cyberterrorism' to facilitate a more effective response to the increasing prevalence of cyber-attacks in the EU (Council of the European Union, 2011b).

The results of this initiative were published four months later in November 2011, wherein the TWP offered the aforementioned glossary of terms on cyber-attacks, which contained the only clear definition of cyberterrorism offered by the EU to-date. Alongside terms such as 'cyberspace', 'cyberspace protection', 'cyber-attack', 'cyber-security', and 'information security incident', the TWP offered the following definition of cyberterrorism as: 'a terrorist offence as defined in the Council Framework Decision 2002/475/JHA committed in cyberspace', with cyberspace limited to the 'digital world of information processing and exchange generated by information and communication technology systems, which includes all aspects of online activity' (Council of the European Union, 2011c). The 2002 framework decision contains a list of eight terrorist offences, with the offence that appears to be most relevant to cyberterrorism being: '(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss' (Council of the European Union, 2002c), although it should be noted that according to the TWP definition all eight offences could be considered cyberterrorism if conducted in 'cyberspace'.

Following its review and glossary of terms, the TWP highlighted that 'cyberterrorism is not clearly defined in any of the Member States'. The TWP also noted that 'the concept of cyber-attack would be used in most cases and cyberterrorism incidents would be treated as acts of terrorism', with little in the way of discernible 'differences in the basic investigational approach to these two concepts', with 'the lack of a coherent terminology at the EU level' translating 'to a lack of state solutions in developing cyberterrorism strategies' (Council of the European Union, 2011c, p. 7). Interestingly, with the TWP having clearly outlined the need for a more coherent terminology with regard to the offence of cyberterrorism, the concept was once again notable by its absence from the new EU Cybersecurity Strategy, released in February 2013 (European Commission, 2013). Cyberterrorism was mentioned just once, with no follow-through on the TWP suggestion that a definition of cyberterrorism should be developed to guide Member State responses to this issue. The document highlighted the issue of cyberterrorism in the context of 'mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy', noting that it was essential that the EU enhanced cooperation 'with international partners and organisations, the private sector and civil society to support global capacity-building in third countries … [in order] to prevent and counter cyber threats, including accidental events, cybercrime and cyberterrorism' (European Commission, 2013).

It is also important to note that the concept of cyberterrorism was only mentioned once in the European Agenda on Security (European Commission, 2015), and not at all in the updated EU Framework Decision on Combating Terrorism (Council of the European Union, 2017) or the EU Cyber Security Act (Council of the European Union, 2019).

Indeed, the European Agenda on Security focused predominantly on the issue of 'cybercrime', with cyberterrorism discussed only briefly as a subset of cybercrime, while the 2019 Cyber Security Act preferred the use of the terms 'cyber threat' or 'cyberattack' as phrases that broadly cover all forms of cybercrime. Interestingly, the Cyber Security Act (European Union, 2019) offers a list of 22 definitions of key terms under Article Two of the act, yet a definition of the term cyberterrorism was, once more, not offered. The fact that the EU has still not offered a clear definition makes the task of inferring how the EU understands cyberterrorism more difficult but not impossible. There are several key sub-strands that help to constitute an EU definition of cyberterrorism.

First, for the EU, cyberterrorism is viewed as one of several hybrid security threats challenging its Member States. As the European Agenda on Security noted, 'threats such as those posed by cyberterrorism and hybrid threats could increase in the years to come' (European Commission, 2015). The concern with hybrid threats has also been invoked in many of the debates on security issues in the European Parliament. For example, in a debate on the 71st Session of the United Nations General Assembly in 2016, Kovatchev claimed that the opportunity to voice the opinion of the EP was of great importance in challenging times, especially when set against 'the conflict on the EU's doorstep, Europe's growing exposure to hybrid warfare, cyberterrorism, foreign fighters, unprecedented waves of migrants, and the blurring of the distinction between external and internal threats' (Kovatchev, 2016). Similarly, Europol has warned of the dangers of 'cyber and terrorism' converging, noting that 'a cyber-attack may amplify the impact of a real-world attack, if carried out in conjunction with the latter, in what may be called a hybrid attack, for example, by disrupting emergency or other essential public services' (Europol, 2018).

Second, the EU discourse on cyberterrorism views it as a new and increasing threat, one that is both borderless and a very real threat to democracy. Europol has been a key institution in articulating this aspect of the perceived threat from cyberterrorism highlighting that member states should be aware that cyberterrorism employs a 'new modus operandi' where 'terrorists are able to operate from remote locations, minimising the risk of detection' (Europol, 2016). Similarly, debates in the European Parliament have mirrored these concerns, with the MEP Gomes having argued that 'cyberterrorism is becoming more sophisticated, cheaper and easier to execute' (Gomes, 2015). Indeed, a European Parliament resolution from 2015 outlined this aspect of the EU cyberterrorism discourse, highlighting that anti-terrorism measures were necessary to 'defend the fundamental values of freedom, democracy and human rights and to uphold international law', with 'cyberterrorism … [enabling] terrorist groups to establish and maintain links without the physical obstacle of borders' (European Parliament, 2015a).

Third, the EU constructs cyberterrorism as a potential future threat, which requires preventative action to be taken in the present. For example, the EU CTC claimed in a report from January 2011 that while in comparison to 'other threats such as cyber espionage and cyber-attacks by organized crime groups or state actors, cyberterrorism has not yet become a key concern … action needs to be taken today to be prepared against a future threat' (Council of the European Union, 2011a). Similarly, the TWP suggestion in 2011 that the EU take steps to develop knowledge on the threat from cyberterrorism was based on the premise that such knowledge would be essential 'to prevent terrorist attacks and enhance the Union and individual Member States' preparedness for future cyberterror

threats' (Council of the European Union, 2011c). Europol (2016) has also highlighted the potential future threat of cyberterrorism, explaining that the 'likelihood of future attacks' being based on 'a stronger cyber dimension' is now a real possibility and that 'terrorists have certainly demonstrated their flexibility and willingness to learn and further develop their technical skills' (Europol, 2016). This invoking of cyberterrorism as a future threat lends credence to de Goede's assertation that the EU's role as a security actor and its emerging 'security culture' is based around the adoption of pre-emptive forms of security practice (de Goede, 2011).

Fourth, it is important to note that the EU often conflates the act of cyberterrorism with the issue of terrorist use of the internet (Argomaniz, 2015). For example, in a speech delivered in 2008 on updating the EU Framework Decision on Combating Terrorism, the MEP Coelho (PPE-DE) suggested that there were over '5,000 terrorist propaganda sites, which are tools of radicalisation and recruitment … [and] a source of information on terrorist means and methods', which should be viewed as a form of 'cyberterrorism' (Coelho, 2008). Similarly, in a letter from the outgoing Lithuanian Presidency of the European Council to the incoming Greek Presidency, the document argued that with regard to 'cyberterrorism … special attention should be paid to the fact that the internet and other network platforms have a central part to play in terrorism threats and radicalisation' (Council of the European Union, 2013).

IV. Securing Critical Infrastructure

Although cyberterrorism has not been conclusively defined, and there is an absence of an incident that might be labelled 'cyberterrorism' per se, we can speak of a loose consensus within cyberterrorism scholarship that a 'cyber-attack' by terrorist entities would entail an attack upon critical infrastructure (see Bieda and Halawi, 2015; Denning, 2000; MacDonald *et al*., 2019). The authors suggest that the threat of cyberterrorism has been invoked across EU institutions as part of a process of re-legitimizing the need for pan-European involvement in the securing of critical infrastructure. Recent official Commission communications have emphasized the increased interdependency between societal and economic functions and the digital technologies that support these; particularly with respect to critical infrastructure (see European Commission, 2017, 2020a, 2020b, 2020c). The Commission has also argued that the SARS-CoV-2 pandemic has increased the risk of hybrid threat actors – including non-state actors such as terrorists – committing politically motivated attacks against key digital systems (European Commission, 2020b; European Commission, 2020c). The EU Commission publications feed into one another and overlap in places, rather than necessarily operating in a vacuum. The communication on the EU Cybersecurity Strategy for the Digital Decade (European Commission, 2020a), for instance, emphasizes that the need to impede terrorist's misuse of cyber tools to plan and execute attacks overlaps with the ambitions of the EU Counter-Terrorism Agenda (European Commission, 2020d).

The concern about the vulnerability of digital interdependency is captured in the following excerpt from the First Progress Report on the EU Security Union Strategy:

> the daily lives of citizens rely on an ever more interconnected and interdependent physical and digital infrastructure. This infrastructure is vital for the functioning of the

> economy and of society. Without reliable supplies of energy, predictable transportation, comprehensive health systems … our current way of life would not be possible. The covid-19 pandemic has shown even more clearly the importance of ensuring the resilience of critical sectors and operators. The EU has recognised the common interest in protecting critical infrastructure from threats, whether natural or man-made disasters, or terrorist attacks. The current threat picture facing critical infrastructure is wide-ranging. It includes: terrorism, hybrid actions, cyber-attacks, insider incidents, threats associated with new and emerging technologies … Our current rules need modernising and expanding (European Commission, 2020c).

Examples of critical infrastructure that could be targeted in a hypothetical cyberterrorist incident include financial systems, energy grids, water supplies and transportation. One of the tenets of the 'Denning approach' to defining cyberterrorism is that it enables stakeholders to distinguish between 'costly nuisances' (for example, the temporary defacement of a webpage) and bona fide 'terror'. Formerly the remit of science fiction, the potential for successful cyber-attacks against critical infrastructure is now public-domain knowledge, with the geopolitically-motivated attacks occurring with the 2009/10 American–Israeli 'Stuxnet' attack against uranium-enrichment centrifuges at Natanz, in Iran and the 2016 attack against utilities in Ivano-Frankivsk Oblast in Ukraine (Goodin, 2016; Williams, 2011). Profit-motivated cyber-attacks have also impacted key systems. Recent ransomware strains in 2020–21 have demonstrated a capacity to either directly or indirectly cause disruption to critical infrastructure and services, including: health service provision in Ireland (Palmer, 2021), council services in Hackney (Sheridan, 2021), beef production in Australia, Canada and the USA (Makortoff, 2021), and the supply of half of the gas consumed in the eastern USA (Wilkie, 2021).

There is no publicly-known instance of proscribed terrorists using malware to cause kinetic disruption to infrastructure. Nonetheless, the linkage between 'cyberterrorism' and the perceived vulnerability of critical infrastructure is exhibited prominently in EU discourse. Furthermore, the correlation between cyberterrorism and vulnerable critical infrastructure pre-dates the tangible case studies mentioned above. Referring to then-recent blackouts in North America and Europe, a 2004 Commission document conjured a hypothetical risk that analogue and digital terrorist activity could be combined, noting that 'cyberterrorism could also result in an amplification of the physical attack's effects', suggesting that damaged communication systems could exacerbate casualty numbers and public panic (European Commission, 2004). A 2009 Commission document arguing for continued cooperation on critical infrastructure protection at the EU-level drew upon the threat of 'terrorist activities targeting critical information infrastructures' to further consolidate the existing Council Framework Decision on Attacks Against Information Systems (European Commission, 2009a). This is a consistent theme exhibited by the EU cyberterrorism discourse. That is, the concern that terrorists might launch successful cyber-attacks against critical infrastructure within a member state or an EU partner is an anticipatory risk aligning with pre-existing or emergent frameworks. The spectre of the cyberterrorist serves to reinforce wider narratives concerning the need to improve and standardize EU-wide approaches to securing critical systems (European Commission, 2009b).

The international public revelation of the successful Stuxnet attack against the 'air-gapped'[1] SCADA system running uranium centrifuges at Natanz marked a step-change in the perceived possibilities of cyber-attacks against critical systems. Although member states would have been conscious of the potential of such attacks – with cyber offence and defence programmes of their own – the Stuxnet incident provided a discursive 'latch'; the first publicly-revealed major cyber-attack causing kinetic damage, driven by geopolitics. The incident provided some legitimacy for commentators to speak of 'cyberterrorism' without resorting to science fiction or conjecture. This sparked a flurry of commentary within the bodies of the EU, with respect to the capacity of cyberterrorists to damage critical infrastructure and cause more general disruption (Council of the European Union, 2010, 2011a).

In an effort to assess the state of the art on countering cyberterrorism across EU membership, in 2011, the European Council produced a document entitled *Summary of the initiative on countering cyber-attacks conducted by terrorists and related entities*, noting that 'such attacks do not currently constitute a high risk' and that the purview of the initiative was to assess levels of preparedness across the Union, the document re-iterated the Council's view that 'cyberterrorism' was a 'terrorist offence as defined in the Council Framework Decision 2002/475/JHA committed in cyberspace' (Council of the European Union, 2011c), in reference to the EU's articulation of terrorist definitions from 2002.

Importantly, the EU's 2002 parameters of 'terrorist' incidents were updated in 2017.[2] This revision maintained the existing parameters – mentioned above – which befit the boundaries of cyberterrorism, but *added* an additional relevant clause, encouraging member states to regard as terrorist activity 'illegal system interference', which urged member states to:

take the necessary measures to ensure that seriously hindering or disrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor (European Parliament, 2013a).

Arguably, a case could be made that some degree of broadening of the term 'cyberterrorism' existed before the 2017 revision; in a 2013 speech delivered at the annual conference of the European Defence Agency, the Herman van Rompuy, the then-President of the Council, remarked 'take for instance terrorism, and cyberterrorism: a potential threat to the arteries of globalised modern life: telecommunication, banking systems, airports or energy grids' (Rompuy, 2013). Although it is apparent that EU discourse on the threat of cyberterrorism has, in part, been fed by the critical infrastructure-oriented case studies elucidated above, much of the discourse on cyberterrorism projected a hypothetical future-facing threat. The EU has spoken in general terms about the *potential* of cyberterrorism to exploit the vulnerabilities in critical infrastructure situated in the EU, necessitating member states to implement best-practice to prevent successful attacks upon their critical infrastructure. Cyberterrorism was regarded as a sufficiently unique threat to warrant mention on several occasions, but, importantly,

[1]An 'air-gapped' system is one that is ostensibly 'offline' and not connected to the world-wide-web. Such air-gapped SCADA systems can, however, still present vulnerabilities due to the necessity of USB and peripheral connection ports, which are required for firmware updates. These ports present an attack vector.
[2]This is the most-recent version.

the threat was raised as a 'package' of risks facing member states in an increasingly diffuse, hybrid context. The authors argue that, for the EU, the 'threat' of cyberterrorism befits a narrative – through discourse and practices – of 'riskification' (see Corry, 2012). Cyberterrorism is posited as a possible risk enabled by the digital interdependence of European society and economics, which, in turn, (re)creates an impetus for EU-driven changes in practice that aim to reduce vulnerability and render risks increasingly governable.

This discursive construction of the vulnerability of critical infrastructure – and its linking to the need to consolidate best-practice – emerged and proliferated from 2012 onwards in debates and in open communiques. For instance, the European Parliament argued that with respect to cyberterrorism and the risk presented to critical infrastructure, there is a requirement for 'new technologies and capabilities' (2013). Two years later, in reference to the Common Security and Defence Policy, the Parliament proposed a need to 'strengthen our capabilities as regards cyberattacks and cyberterrorism', and that the Action Plan would 'mark the beginning of a move towards the more systematic integration of cyber defence issues among the institutions of the EU', including 'a coherent European strategy to secure critical infrastructure against cyberattacks' (European Parliament, 2015b). A later Parliament resolution referred to the 'online propaganda and cyber attacks' conducted by Islamic State affiliates, that bolstered not only the need for greater EU cooperation with external partners to prevent cyber threats including cyberterrorism, but also the EU's normative case for the internet's core infrastructure to be a 'neutral zone' (European Parliament, 2016).

Similarly, a Parliament resolution published in June 2018 reported that the EU faced an unprecedented convergence of threat, including the development of 'cyber arms to wage cyberterror campaigns, to disrupt, damage or destroy critical infrastructure, to attack financial systems and to pursue other illegal activities that have implications for the security of European citizens' (European Parliament, 2018a). The authors of the resolution urged for the implementation of three distinct practices. Notable from these was that member states should anticipate that bilateral agreements with other states would not be as effective as the EU cooperating multilaterally – as a unified entity – with external partners 'to tackle the challenges posed by cyberterrorism and by cryptocurrencies and other alternative payments of methods' (European Parliament, 2018a).

There is therefore a sense that the European Parliament communiqués complemented and ascribed further legitimacy to the arguments put forward by the Commission and Council, with no dissent. The anticipatory threat of cyberterrorism befitted the EU's view of a broadened threat horizon implicated by the linkage between cyberspace and critical systems. The vulnerability of these systems was seen in the light of an increasing prominence of 'hybrid' threats and new forms of terrorism 'among them cyberterrorism' (European Parliament, 2018b). This particular construction of perceived hybrid threat was underpinned by a multiplicity of both *actors* and *vectors* of attack. That is, the suggested synergy between criminal organizations and terrorist groups had led to a situation in which cyber-attack tools developed by organized crime could be wilfully repurposed by terrorist organizations to target critical infrastructure for political purposes. This warranted both greater impetus for existing cooperation within and beyond the EU, including with regard to securing critical infrastructure, accommodating best cyber-security

practice, consolidating policing networks between member states, and the pushing of an EU-wide narrative with respect to cyberspace 'norms'.

Conclusion

Through the engagement that EU institutions have invested with the phenomenon of cyberterrorism from 2002 onwards, the EU has positioned itself as a forefront actor in the ongoing discursive construction of the converging threats posed by cyber-weaponry and extremism. Generally, the EU's discourse on cyberterrorism ascribes it with meaning akin to that deployed elsewhere; that is to say, cyberterrorism is regarded as epitomizing the fear that terrorists could intentionally target critical infrastructure systems via remote electronic means. It was apparent that the EU's construction of the threat of cyberterrorism relates to the idea that the threat of cyberterrorism is part of a *basket of threats* that warrants a legitimization of pre-existing, current and future practices for the securing of critical infrastructure both within the EU itself and indeed further afield. This is emblematic of a broader trend that has been identified elsewhere within the EU's perspective on the cyber-threat landscape. In particular, we may characterize the institutions of the EU as regarding the act of cyber-*attack* of significance, irrespective of the *source*. So, the securitisation of the threat of cyberterrorism on the basis of this threat basket befits a catch-all approach to increasing the resilience of critical infrastructure to cyber-interference. This approach to articulating the cyber-threat landscape is also emblematic of a preventative approach to mapping and mitigating the risks facing critical systems within member states. The EU's narration of the threat of cyberterrorism consciously straddles both the counter-terrorism agenda and the cybersecurity strategy. The threat is raised – amongst other state and non-state threats – as a rallying call for a continued rollout of existing proposals, as well as a rationale for discussions around new proposals. These practices include (amongst others) the endorsement of the Budapest Convention, the sharing of data between law enforcement and other parties, the standardization of IT security practices, EU-level collaboration with third party countries, and raising the resilience of supply chains. The EU is self-projected not as a norm-taker, but as a lead agent in reducing the vulnerability of digital interconnectivity against a diffuse range of threat actors, including terrorists.

Although this article has focused on the various ways in which the EU has sought to define cyberterrorism and the linkage of this threat to the vulnerability of critical systems, there were additional strands identified through the interpretive discourse analysis that warrant further scrutiny. In particular, other strands of the discourse on cyberterrorism not discussed here include: the idea that cyberterrorism was a threat deemed to be increasing in both likelihood and potential severity; concern that cyberterrorism is a complex hybrid threat; fear that societal pillars including 'democracy' and 'freedom' were themselves at risk from the threat of cyberterrorism; and the discursive elucidation of this threat as part of broader arguments about the need for further European integration. Future research could also investigate in greater detail a comparison between the EU's construction of cyberterrorism vis-à-vis that of other actors such as the USA or the UK.

Nonetheless, it is of note that despite a flurry of activity in 2011 with respect to the apparent need to define cyberterrorism, this drive did not last. The EU is not alone in this regard, as the British securitisation of the threat of cyberterrorism also reflected a degree

of cautiously cultivated ambiguity. To some extent, this broader trend may be fed by the absence of an incident that we can clearly understand to be an instance of cyberterrorism per se. Arguably, there is a need for the EU to return to the debate that it had commenced in 2011, and follow through with criteria and definitions that define cyberterrorism, differentiated from general use of the internet by terrorists. This is a narrative not only about hypothetical terrorist hands behind keyboards (Mott, 2019), but also about the standing and outlook of the EU as a leading international authority in cyber-crime and responses to diffuse security threats. There is a case to build upon the success of the Budapest Convention[3] in the establishment of the EU as both a 'hub' and a leading authority for collaborative cyber security. In constructing threats via the discursive platforms of its respective institutions, the EU itself engages in an ongoing process of articulating its own unique security role within a threat environment that is simultaneously national, regional and global.

Correspondence:
Christopher Baker-Beall, Disaster Management Centre, Bournemouth University, Bournemouth, UK.
email: cbakerbeall@bournemouth.ac.uk

References

Argomaniz, J. (2011) *Post-9/11 European Counter-Terrorism Politics* (London: Routledge).
Argomaniz, J. (2015) 'European Union Responses to Terrorist use of the Internet'. *Cooperation and Conflict*, Vol. 50, No. 2, pp. 250–68.
Ashley, R. (1988) 'Untying the Sovereign State: A Double Reading of the Anarchy Problematique'. *Millennium*, Vol. 17, No. 2, pp. 227–62.
Baker-Beall, C. (2014) 'The Evolution of the European Union's 'Fight Against Terrorism' Discourse: Constructing the Terrorist "Other"'. *Cooperation and Conflict*, Vol. 49, No. 2, pp. 212–38.
Baker-Beall, C. (2016) *The European Union's Fight Against Terrorism* (Manchester: Manchester University Press).
Balzacq, T. *et al*. (2010) Security Practices, *Oxford Research Encyclopedia of International Studies*.
Bevir, M., Daddow, O. and Hall, I. (2013) 'Introduction: Interpreting British Foreign Policy'. *British Journal of Politics and International Relations*, Vol. 15, No. 2, pp. 163–74.
Bieda, D. and Halawi, L. (2015) 'Cyberspace: a Venue for Terrorism'. *Issues in Information Systems*, Vol. 16, No. 3, pp. 33–42.
Bigo, D. (2007) *Policing Insecurity Today: Defence and Internal Security* (London: Palgrave Macmillan).
Boin, A., Rhinard, M. and Ekengren, M. (2014) 'Managing Transboundary Crises: The Emergence of European Union Capacity'. *Journal of Contingencies & Crisis Management*, Vol. 22, No. 3, pp. 131–42.
Bossong, R. (2012) *The Evolution of EU Counter-Terrorism: European Security Policy after 9/11* (London: Routledge).

[3]The Council of Europe Convention on Cybercrime – also known as the Budapest Convention – boasting 64 signatories and nine observers, stands as the only legally binding instruments providing a framework on international cooperation against cyber-crime (Pawlak, 2019; Council of the European Union, 2021).

Bures, O. (2011) *EU Counterterrorism Policy: Terrorist Threats and the European Union's Responses* (London: Routledge).
Carrapiço, A. and Barrinha, A. (2017) 'The EU as a Coherent (cyber)Security Actor?' *Journal of Common Market Studies*, Vol. 55, No. 6, pp. 1254–72.
Christou, G. (2018) 'The Challenges of Cybercrime Governance in the European Union'. *European Politics and Society*, Vol. 19, No. 3, pp. 355–75.
Christou, G. (2019) 'The Collective Securitisation of Cyberspace in the European Union'. *West European Politics*, Vol. 42, No. 2, pp. 278–301.
Christou, G. and Simpson, S. (2011) 'The European Union, Multilateralism and the Global Governance of the Internet'. *Journal of European Public Policy*, Vol. 18, No. 2, pp. 241–57.
Coelho, C. (2008) Combating Terrorism – Protection of Personal Data. European Parliament. A6-0322/2008.
Conway, M. (2008) *'Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures, School of Law and Government'*. (Dublin City University Working Paper No. 5).
Corry, O. (2012) 'Securitisation and "Riskification": Second-order Security and the Politics of Climate Change'. *Millennium: Journal of International Studies*, Vol. 40, No. 2, pp. 235–58.
Council of the European Union (2002a) 10th EU–Japan Summit. 10 January. 15175/01.
Council of the European Union (2002b) Non-confidential Report on the Terrorism Situation and Trends in Europe. 20 November. 14280/02.
Council of the European Union (2002c) Council Framework Decision of 13 June 2002 on Combating Terrorism.
Council of the European Union (2005a) 'EU Counter-Terrorism Strategy'.
Council of the European Union (2005b) Council Framework Decision 2005/222/JHA on Attacks Against Information Systems.
Council of the European Union (2006) Implementation of the Action Plan to Combat Terrorism. 19 May. 9589/06.
Council of the European Union (2010) 'EU Counter Terrorism Strategy'. Discussion Paper.
Council of the European Union (2011a) EU Action Plan on Combating Terrorism. 17 January. 15893/1/10.
Council of the European Union (2011b) Summary of Discussions. Working Party on Terrorism. 25 July. 13185/11.
Council of the European Union (2011c) Summary of the Initiative on Countering Cyber Attacks Conducted by Terrorists and Related Entities. Working Party on Terrorism. November. 17675/1.
Council of the European Union (2013) Letter from the LT Presidency to the Incoming EL Presidency on the Future Development of the JHA Area. 13 December. 17808/13.
Council of the European Union (2017) Directive on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA. 2015/0281.
Council of the European Union (2019) Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
Council of the European Union (2021) Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Available at: https://www.coe.int/en/web/cybercrime/parties-observers. Last accessed 18 February 2021.
de Goede, M. (2011) *European Security Culture: Pre-emption and Precaution in European Security* (Amsterdam: University of Amsterdam).
de Londras, F. and Doody, J. (2015) *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism* (Abingdon: Routledge).

Denning, D. (2000) Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives. 23 May.
Eling, K. (2007) 'The EU, Terrorism and Effective Multilateralism'. In Spence, D. (ed.) *The European Union and Terrorism* (London: John Harper).
European Commission (2001) 'EU Response to the 11 September: European Commission Action. 3 June. Memo/02/122'.
European Commission (2004) *Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight against Terrorism. 20 October.*
European Commission (2009a) Critical Information Infrastructure Protection. 30 March.
European Commission (2009b) Justice, Freedom and Security in Europe since 2005: An Evaluation of the Hague Programme and Action Plan. 10 June.
European Commission (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7 February.
European Commission (2015) The European Agenda on Security. 28 April.
European Commission (2017) Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. 13 September.
European Commission (2020a) The EU's Cybersecurity Strategy for the Digital Decade. 16 December.
European Commission (2020b) Communication on the EU Security Union Strategy. 24 July.
European Commission (2020c) First Progress Report on the EU Security Union Strategy. 9 December.
European Commission (2020d) A Counter-Terrorism Agenda for the EU. 9 December.
European Parliament (2011) Report on EU Counterterrorism Policy: Main Achievements and Future Challenges.
European Parliament (2013a) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA.
European Parliament (2015a) European Parliament Resolution of 11 February 2015 on Anti-terrorism Measures. 2015/2530(RSP).
European Parliament (2015b) European Parliament Resolution of 21 May 2015 on the Implementation of the Common Security and Defence Policy 2014/2220(INI).
European Parliament (2016) European Parliament Resolution of 14 December 2016 on the Implementation of the Common Foreign and Security Policy 2016/2036(INI).
European Parliament (2018a) European Parliament Resolution of 13 June 2018 on Cyber Defence 2018/2004(INI).
European Parliament (2018b) European Parliament Resolution of 12 December 2017 on Findings and Recommendations of the Special Committee on Terrorism 2018/2044(INI).
European Union. (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
Europol (2016) TE-SAT: EU Terrorism Situation and Trends Report. 20 July.
Europol (2018) TE-SAT: EU Terrorism Situation and Trends Report. 20 July.
Eurostat (2019) Digital Economy and Society to Statistics – Households and Individuals. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access. Last accessed 19 January 2021.

Fahey, E. (2014) 'The EU's Cybercrime and Cyber Security Rulemaking: Mapping the Internal and External Dimensions of EU Security'. *European Journal of Risk Regulation*, Vol. 5, No. 1, pp. 46–60.
Gomes, A. (2015) Cyber-attacks Against the Media – New Level of Threat to Cybersecurity. European Parliament. 27 May. 2015/2709(RSP).
Goodin, D. (2016) 'Analysis Confirms Coordinated Hack Attack Caused Ukrainian Power Outage'. *Arstechnica*, 11 January. Available at: http://arstechnica.com/security/2016/01/analysis-confirms-coordinated-hack-attack-caused-ukrainian-power-outage/
Guitton, C. (2013) 'Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?' *European Security*, Vol. 22, No. 1, pp. 21–35.
Hassan, O. (2010) 'Constructing Crises, (in)Securitising Terror: The Punctuated Evolution of EU Counter-Terror Strategy'. *European Security*, Vol. 19, No. 3, pp. 445–66.
Jackson, R. (2007) 'The Core Commitments of Critical Terrorism Studies'. *European Political Science*, Vol. 6, No. 3, pp. 244–51.
Kaunert, C. (2010) 'Towards Supranational Governance in EU Counter-Terrorism? The Role of the Commission and the Council Secretariat'. *Central European Journal of International and Security Studies*, Vol. 4, No. 1, pp. 8–31.
Kovatchev, A. (2016) 71st Session of the UN General Assembly, European Parliament, 6 July. 2016/2020(INI).
Larsen, H. (2002) 'The EU: A Global Military Actor?' *Cooperation and Conflict*, Vol. 37, No. 3, pp. 283–302.
MacDonald, S., Jarvis, L. and Lavis, S. (2019) 'Cyberterrorism Today? Findings from a Follow-on Survey of Researchers'. *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610X.2019.1696444
MacKenzie, A., Kaunert, C. and Leonard, S. (2014) 'Counter-Terrorism: Supranational EU Institutions Seizing Windows of Opportunity'. In Trauner, F. and Servent, A. (eds) *Policy Change in the Area of Freedom, Security and Justice* (London: Routledge), pp. 109–29.
Makortoff, K. (2021) 'World's Biggest Meat Producer JBS Pays $11m Cybercrime Ransom'. *The Guardian*. Available at: https://www.theguardian.com/business/2021/jun/10/worlds-biggest-meat-producer-jbs-pays-11m-cybercrime-ransom. Last accessed 14 September 2021.
Mott, G. (2019) *Constructing the Cyber Terrorist* (London: Routledge).
Palmer. D. (2021) 'Ransomware: Ireland's Health Service Remains "Significantly" Disrupted Weeks after Attack'. *Znet*. Available at: https://www.zdnet.com/article/ransomware-irelands-health-service-is-still-significantly-disrupted-weeks-after-attack/. Last accessed 14 September 2021.
Pawlak, P. (2019) 'The EU's Role in Shaping the Cyber Regime Complex'. *European Foreign Affairs Review*, Vol. 24, No. 2, pp. 167–86.
Rees, W. (2008) 'Inside Out: The External Face of EU Internal Security Policy'. *European Integration*, Vol. 30, No. 1, pp. 97–111.
Renard, T. (2018) 'EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain'. *European Politics and Society*, Vol. 19, No. 3, pp. 321–37.
Rompuy, H. (2013) 'Defence in Europe: Pragmatically Forward'. Speech by President of the European Council Herman van Rompuy at the Annual Conference of the European Defence Agency.
Ruohonen, J., Hyrynsalmi, S. and Leppanen, V. (2016) 'An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus'. *Government Information Quarterly*, Vol. 33, pp. 746–56.
Sheridan, E. (2021) 'Cyber Attack: Hundreds of Residents still Facing Disruption with Benefits Payments'. *Hackney Citizen*. Available at: https://www.hackneycitizen.co.uk/2021/03/19/

cyber-attack-hundreds-residents-disruption-benefits-payments/. Last accessed 14 September 2021.
Sliwinski, K. (2014) 'Moving Beyond the European Union's Weakness as a Cyber-Security Agent'. *Contemporary Security Policy*, Vol. 35, No. 3, pp. 468–86.
Sperling, J. and Webber, M. (2019) 'The European Union: Security Governance and Collective Securitisation'. *West European Politics*, Vol. 42, No. 2, pp. 228–60.
Tsoukala, A. (2004) 'Democracy Against Security: the Debates about Counterterrorism in the European Parliament, September 2001–June 2003'. *Alternatives*, Vol. 29, No. 4, pp. 417–39.
Wilkie, C. (2021) 'Colonial Pipeline Paid $5 million Ransom One Day after Cyberattack, CEO tells Senate'. *CNBC*. Available at: https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html. Last accessed 14 September 2021.
Williams, C. (2011) 'Stuxnet: Cyber Attack on Iran "Was Carried out by Western Powers and Israel"'. *The Telegraph*, 21 January. Available at: http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html
Wittendorp, S. (2016a) 'Unpacking "International Terrorism" Discourse, the European Community and Counter-Terrorism, 1975–1986'. *JCMS*, Vol. 54, No. 5, pp. 1233–49.
Wittendorp, S. (2016b) 'Conducting Government: Governmentality, Monitoring and EU Counter-Terrorism'. *Global Society*, Vol. 30, No. 3, pp. 465–83.
Zwolski, K. (2012) 'The EU as an International Security Actor after Lisbon: Finally a Green Light for a Holistic Approach?' *Cooperation and Conflict*, Vol. 47, No. 1, pp. 68–87.