The New EU Counter-Terrorism Agenda: Preemptive Security through the Anticipation of Terrorist Events

Christopher Baker-Beall[1] and Gareth Mott[2]

Abstract

This article argues that the new Counter-Terrorism Agenda for the EU is based on logics of anticipatory action. Building on research by Ben Anderson, three types of anticipatory action are identified: preparedness, precaution and preemption, which it is argued have been central to the development of EU counter-terrorism policy. We contend that while the original EU Counter-Terrorism Strategy contained a mixture of the three forms of anticipatory action identified by Anderson, the new Counter-Terrorism Agenda places a renewed emphasis on preemptive counter-terrorism measures as central to the EU's evolving strategy in this area, with the notion of preparedness given less prominence. It is argued that the reinforcing of preemptive security practice is most vividly reflected in the CT Agenda's new Anticipate workstream, which emphasises the utility of new preemptive computer-based technologies, including Artificial Intelligence and Algorithms, as a key dimension of the EU's response to terrorism. The article identifies challenges of transparency and effectiveness that arise when applying new computer-based technologies to counter-terrorism, highlighting the importance of regulatory oversight if the EU's commitment to the development of security policies that respect fundamental rights is to be guaranteed.

Introduction

The new European Union (EU) Counter-Terrorism Agenda (European Commission, 2020), released in December 2020, offers the first major update to the European Counter-Terrorism Strategy in over 15 years (Council of the EU, 2005). The original EU CT Strategy, released in 2005, was modelled on the United Kingdom's (UK) CONTEST counter-terrorism strategy (UK Government, 2004). What is interesting about both the UK and the EU counter-terrorism strategies, which is not often remarked upon, is that they are actually emergency planning documents (Omand, 2012; Hardy, 2015). The original UK CONTEST Strategy was launched as a confidential document authored by Sir David Omand, in November 2002, as part of a drive by the Cabinet Office to ensure risk assessment and risk management were built into domestic security planning by the UK government (Omand, 2012). The UK strategy was underpinned by a strategic aim of reducing the risk from terrorism, through enhancing the preparedness and resilience of the UK to terrorist attacks.

A similar rationale involving the need for risk assessment and risk management also underpinned the EU's initial CT Strategy. The European Commission's (2004) communication on terrorist attacks, which set the ground for the 2005 CT Strategy, also revolved around key principles from the field of emergency planning (see Alexander, 2002). The document explained that 'effective prevention, preparedness and response of the Union to terrorist attacks are overarching objectives' of the effort to combat terrorism (Commission, 2004). The EU CT Strategy (Council of the EU, 2005) was released in November 2005 and like the UK CONTEST Strategy, was based on four workstreams: Prevent, Protect, Pursue and Respond. However, the EU document used the term Respond rather than Prepare (UK

[1] Disaster Management Centre, Bournemouth University | cbakerbeall@bournemouth.ac.uk
[2] School of Politics and International Relations, University of Kent | g.mott@kent.ac.uk

Government, 2004). With respect to the focus of each workstream: Prevent concerns the EU's counter-radicalisation strategy, which is designed to prevent people from being drawn into terrorism; Protect involves reducing vulnerability to terrorist incidents through improved security of borders, transport and critical infrastructure; Pursue focuses on the disruption of terrorist activities, including the funding of terrorism; while Respond emphasises the importance of improving coordination of the response to terrorism and enhancing resilience in the aftermath of an attack (Council of the EU, 2005).

The original EU CT strategy was based on the logics of what is referred to as *anticipatory action* (Anderson, 2010), adopting principles from the field of emergency planning and emphasising the importance of *preparedness* for terrorist attacks (Council of the EU, 2005). The new EU CT Agenda (European Commission, 2020a), like the previous strategy, also includes four workstreams: Anticipate, Prevent, Protect and Respond, with Pursue replaced by the new Anticipate workstream. In the original strategy Pursue involved intelligence-sharing between member states, measures that target the financing of terrorism, the creation of frameworks for joint threat assessment, judicial cooperation, police cooperation and exchange of information, including through the continued development of immigration management databases such as the Visa Information System (VIS) and the Schengen Information System (SISII), and measures targeting communications, all for the purpose of combating terrorism. In the new agenda, the Anticipate workstream retains some of the features of Pursue, such as intelligence sharing and joint threat assessment, with issues like terrorist financing, information exchange, and police and judicial cooperation moving to the Respond workstream.

To date, research on EU counter-terrorism has predominantly analysed the development of policy in this area from historical-institutionalist or public-policy making perspectives (Argomaniz, 2011, Bossong, 2012; Bures, 2011; Kaunert, 2010). A particular area of focus has been the extent to which the EU can be considered an 'international' or 'global' counter-terrorism actor (Monar, 2015: Brattberg and Rhinard, 2012), which builds on the extensive literature on EU actorness (Bretherton and Vogler, 2005) in the field of foreign policy (Larsen, 2002) and more recently the notion of the EU as a 'holistic' security actor (see Zwolski, 2012' Baker-Beall, 2016). Similarly, a smaller body of research has adopted a social-constructivist lens to investigate the role of threat perception (Bakker 2006; Monar 2007; Meyer 2009) or applied interpretive and critical approaches that emphasise the important role of identity, discourse and technologies of governance (Baker-Beall, 2014; Wittendorp, 2016a and 2016b), in the evolution of policy in this area. Additionally, there is a literature on EU security policy more broadly, taking EU responses to terrorism as its subject, which draws insights from Political Sociology and Political Geography. Research developed from this perspective emphasises the relationship between insecurity, risk and anticipatory action in the EU's ongoing development as a security actor (see for example, Bigo, 2008; de Goede, 2008, 2011; Amoore and de Goede, 2012).

Given that it was only released in December 2020, there has yet to be research on the EU's new CT Agenda and specifically the new Anticipate workstream. In order to analyse the new EU CT Agenda, we draw insights from all of the literature on EU counter-terrorism cited above but situate out argument specifically within the literature on insecurity, risk and anticipatory action (de Goede, 2008, 2011; Anderson, 2010), in order to offer a first attempt at analysing the logics that underpin the new EU CT Agenda. As such, we put forward two main arguments. First, that although the new CT Agenda embraces an anticipatory security logic, there is a reorientation away from the principles of preparedness and emergency

planning that were a prominent feature of the first EU CT Strategy, towards an increased focus on precautionary or preemptive counter-terrorism measures. This is not to argue that the focus on preemptive or precautionary security practice is a new or novel dimension of EU counter-terrorism. As we explain below, preemption is most apparent in the Prevent workstream of the EU CT strategy and also the measures designed to combat the financing of terrorism contained in the Pursue workstream. Rather it is to highlight that, as EU counter-terrorism has evolved, this ongoing process reflects a trend towards the adoption of ever more preemptive forms of security as characterised by the new Anticipate workstream.

Indeed, this concern with preemption can be identified in the rationale for the new CT Agenda, which states clearly that the EU needs to be better able to '*anticipate existing and emerging threats* in Europe' (Commission, 2020a: p.3, emphasis added). An essential dimension of this includes the development of 'information sharing and a culture of cooperation', which is viewed as essential to 'solid threat assessment that can form the basis of *a future-proof* counter-terrorism policy', and the use of new technologies to process and evaluate data that might help to prevent the potential terrorist attacks of the future (Ibid, emphasis added). Second, we argue specifically that the EU's focus on new technological solutions, including data mining and profiling of terrorist suspects through the use of Artificial Intelligence (AI) and algorithms, as an essential dimension of the response to counter-terrorism, are not without consequence and entail wider implications for the fundamental rights of EU citizens.

To make this argument the article is broken into four sections. The first section introduces the idea of the EU as an 'Anticipatory Security Actor'. Here we build on the work of Ben Anderson (2010) and outline what is meant by the term *anticipatory* in the context of security, highlighting the similarities and differences that exist between three types of anticipatory action: preparedness, precaution and preemption, all of which can be identified within both the EU Counter-Terrorism Strategy and Counter-Terrorism Agenda for the EU (Council of the EU, 2005; 2020). Second, we identify the threat discourses invoked by the EU to justify the continued development of its counter-terrorism policies. Third, we focus specifically on the Anticipate workstream in the new CT Agenda, demonstrating how it reflects the EU's ever-increasing embrace of preemptive forms of security. Fourth, we consider the potential political and social consequences of the Anticipate workstream, including what it means for the EU's proposed commitment to developing counter-terrorism policies with respect for the fundamental rights of EU citizens.

Before moving forward, a short note on methodology. To achieve its aims, the article applies an interpretive approach to the study of EU counter-terrorism (see Bevir, Daddow and Hall, 2013). This interpretive methodology revolves around a double-reading strategy (see Ashley, 1988; Shepherd, 2008). A first reading identifies the key themes underpinning the discourse. A second reading highlights the relationship between the discourse and the practices that are subsequently enabled as a result. The core focus of the analysis centres upon the new CT Agenda document (Council of the EU, 2020), with additional contextual data drawn from wider EU security documents, including the original EU Counter-Terrorism Strategy (Council of the EU, 2005). The authors also develop critical reflections grounded in the academic literature to assess the implications of the new CT Agenda with respect to security policy.

Having assembled this corpus of EU security documents, the first stage of the interpretive discourse analysis sought to map the discourse, particularly that expressed in the CT Agenda.

This was achieved by asking a series of questions, which were applied to the source material. The first question was "what are the keywords, terms, phrases, labels, metaphors and assumptions in each source?". The second question was "what are the key strands that make up the discourse?". The last 'mapping' question was "how does the discourse construct terrorism as a threat that can be – or should be – anticipated?". Importantly, when answering this question, we used the three types of anticipatory action identified by Anderson (2010) - preparedness, precaution and preemption - to assess the response to terrorism outlined in the EU policy documents.

The final stage of analysis developed a more in-depth understanding of the logic of the discourse. This entailed a second-reading of the sources, applying a further three questions. In order to identify points of partial fixation, the authors asked, "how does the discourse establish knowledge and understanding of future terrorist threats?". The authors then asked a second question designed to reveal the linkage between the threat discourse and the practices that this served to justify, "how is the role of the EU as a security actor legitimised and delegitimised by the articulation of future terrorist threats?". A final question was then applied to the sources, "to what extent did the articulation of the terrorist threat and counter-terrorism practices represent continuity or change in EU security policy?". This question sought to identify the extent to which the CT Agenda either diverged from existing policy, (re)legitimised existing policy, or established a discursive foundation for new policy. The following sections of this article outline the results of this analysis.

The EU as an Anticipatory Security Actor: Preparedness, Precaution and Preemption in the EU Counter-Terrorism Strategy

Since the events of September 11, 2001, the EU has continually sought to develop its capacity as an actor in the field of security. Marieke de Goede (2011) has argued that the EU's emerging *security culture* is characterised by a commitment to 'prevention, anticipation and early intervention' in crisis and conflict. As the first European Security Strategy, released in 2003, states, the EU views its role as a security actor to 'be ready to act *before* a crisis occurs… prevention cannot start too early' (European Council, 2003: 8, emphasis added). Likewise, in the aftermath of the Madrid terrorist attacks in March 2004, the European Commission (2004: 5) released a communication emphasising the need for an integrated approach to 'prevention, preparedness and response' with respect to terrorist attacks. Similar ideas can be found in the 2010 EU Internal Security Strategy, which highlighted the importance of 'prevention' of terrorism and a necessity 'to stay ahead of the threat with a coherent European approach' (European Commission, 2010: 8). For de Goede (2011), although prevention and preparedness are central to EU security policy, it is an embrace of the precautionary principle, that has defined the European approach to contemporary security threats.

The precautionary principle was first outlined in a communication from the European Commission (2000), at the turn of the twenty-first century, in the context of responding to the threat from climate change. In essence, this is the idea that it is important to address threats before they fully emerge. The principle is based on the logic of risk assessment. It recognises that policy-makers are often confronted with situations where normal risk assessments may be difficult or impossible due to a lack of scientific knowledge but where the danger or threat is considered to be high (de Goede, 2011). In such situations, the precautionary principle allows action in the face of scientific uncertainty to overcome perceived threats. Whereas the original intention of this principle was to foster action to prevent the worst impacts of

environmental degradation resulting from climate-change, the EU began to embrace the precautionary logic when responding to security threats, like terrorism, in the period after the Madrid attacks in 2004. Specifically, the focus of the EU's precautionary approach to security is the need to address 'threats and dangers that are irregular, incalculable, and, in important ways, unpredictable' (Ibid: 9).

Although we agree with de Goede that precaution is a key feature of the emerging European security culture, we argue that there are nuances to this approach, with EU security policy, and specifically the original EU CT Strategy, reflecting a mix of the notion of preparedness, which is drawn from the field of Disaster Management (i.e., emergency planning), the precautionary principle and the logics that underpin preemptive approaches to security. The concepts are similar in the sense that preparedness, precaution and preemption are forms of what can be termed *anticipatory* action. In essence, they are best thought of as principles or logics that can act as guidelines for government policy and, importantly, they all share a similar problem: how to act in relation to uncertain futures. As Anderson explains (2010: 778), a common characteristic of all forms of anticipatory action is 'a paradox whereby a future becomes cause and justification for some form of action in the here and now'. Importantly, there are slight differences between each of these concepts, which we will now outline, using the measures contained in the original CT Strategy as a way of demonstrating these differences.

According to Anderson (2010: 791), 'preparedness is different' from precaution and preemption in a specific way. Whereas preemption and precaution are principles that focus on action to be taken to prevent uncertain futures from occurring, 'preparedness does not aim to stop a future event happening' but instead aims to ensure that plans are in place to mitigate against the worst consequences of an event when it inevitably occurs (Ibid). 'Preparedness' is one of the guiding principles of the field of Disaster Management and is interlinked with the concept of 'resilience', meaning an ability to return to an original state or to recover quickly (Alexander, 2015; Zebrowski, 2015). In the original EU CT Strategy, the need for preparedness was most evident in the Respond workstream. The strategy clearly stated that 'the response to an incident will often be similar whether that event is natural, technological or man-made' and, therefore, the response systems used to mitigate against 'natural disasters may also be used to alleviate the effects on citizens in the aftermath of a terrorist attack' (Council of the EU, 2005: 15). Specifically, the strategy identified measures to enhance preparedness, including the development of the EU's crisis coordination arrangements and Civil Protection Mechanism, as essential to an effective response to terrorist attacks when they do occur. Interestingly, measures that enhance preparedness appear to have been either dropped or removed from the new EU CT Agenda (Council of the EU, 2020), which as we argue, places an increased emphasis on the need for preemptive counter-terrorism measures.

The precautionary approach, by way of contrast to preparedness, begins once a threat has been identified, even if there is a degree of scientific uncertainty over the extent of the threat. The purpose of anticipatory action in this context is to act before a threat has reached the point of irreversible damage. The way in which precautionary action is evaluated involves cost-benefit analyses, (e.g., of the future cost of not acting in the present), grounding precaution as a form of rational action. In the original EU CT strategy (Council of the EU, 2005), measures designed to ensure increased cooperation with regard to intelligence sharing and joint threat assessment, dealt with under the Pursue workstream, reflect the logics that underpin a precautionary approach to security. Similarly, the measures outlined under the Protect workstream, aimed at enhancing border security and reducing the vulnerability of

critical infrastructure, including transport and aviation, are all based on a similar precautionary security logic. They are about acting in response to known threats before they are fully realised.

Preemption, by way of contrast to precaution, is slightly different. Although preemption and precaution share similar characteristics, such as the need to act in the present to prevent the actualisation of future threats, there is something markedly different between both concepts as a principle that can provide a framework for policy action. As Leese (2014: 498) explains, preemption involves venturing 'even further into the unknown'. Whereas precautionary action is exemplified by stopping a known threat before it reaches a point of irreversibility, preemption involves action to prevent imagined futures. Preemption provides both a logic and justification for action in the present *before* threats *have even begun* to emerge. The key difference between precaution and preemption as principles that underpin anticipatory action is, therefore, the extent to which we imagine the future (see Leese, 2014).

Preemption in the context of counter-terrorism is framed through the imagination of possible terrorist futures, which provide a circular self-justifying logic. As de Goede (2008a: 160) explains, not only are future terrorist events imagined as if they were real, but they simultaneously demand 'new methodologies of calculation and imagination', in the form of evermore novel counter-terrorism measures, to pre-empt and prevent the events from occurring. However, the need for action is generated not just by the imagining of potential future terrorist events but also because there is an 'assumption that the responsible institutions are guilty if they do not detect the presence, or actuality, of a danger even before it is realized' (Ewald, 1994: 221–2). In the EU CT strategy, the logics of preemption play out in two key areas.

First, through the counter-radicalisation measures contained in the Prevent workstream of the EU CT Strategy, which aims to combat the issue of 'violent radicalisation', i.e., 'the phenomenon of people embracing opinions, views and ideas which *could lead* to acts of terrorism' (European Commission, 2005: 2 emphasis added). Specifically, the aim of this dimension of EU counter-terrorism policy is to bring together governmental and civil society actors, at local, regional, national and the European level, to work together to, preemptively. prevent people from being drawn into terrorism. As de Goede and Simon (2013) explain, the purpose of counter-radicalisation in practice is to 'is to anticipate threat and enable intervention at the earliest possible stage' through 'early identification and intervention in the lifeworlds of potential future radicals'. In essence, the purpose of these preemptive measures is not only to try and identify behaviours that might indicate an individual is on a pathway towards one day becoming a terrorist threat, but to detect terrorists before an individual has even thought of becoming one.

Second, in the new forms of 'dataveillance' created by the EU for the purpose of combating terrorism (Amoore and de Goede, 2005), including the use of databases such as the VIS, the second-generation SIS II and the Criminal Record Information System. In the original EU CT strategy, the measures targeted at the financing of terrorism, located under Pursue, were the clearest example of techniques underpinned by a preemptive security logic. As de Goede has explained, the steps taken by the EU to monitor financial transactions and freeze the assets of terrorist suspects are, like counter-radicalisation measures, also preemptive; they allow extra-legal intervention before an offence has been committed, criminalising everyday financial activities on the basis of an imagined future where an individual may (or may not) become a terrorist (de Goede, 2008b).

We argue that although each of the workstreams that constitute the new CT Agenda for the EU reflect elements of preparedness, precaution and preemption, the EU is moving further towards the embrace of a preemptive security logic in the development of policy in this area, reinforcing the logics that underpin the EU counter-terrorism measures that deal with radicalisation and the financing of terrorism, with the Anticipate workstream most vividly reflecting this move. Of course, in order to justify the preemptive measures outlined under Anticipate, the EU has to invoke the imagined terrorist threats of the future. The next section therefore outlines some of the terrorism threat narratives, which according to the EU, make these developments a necessity.

Terrorism Threat Discourses

The invoking of the threat from terrorism to justify the development of the EU's capabilities as a security actor is not new. The initial steps taken towards European internal security cooperation with the creation of the Trevi structure in the 1970s were accompanied by a narrative that proclaimed the threat from 'international terrorism' made coordination of policy necessary (Baker-Beall, 2013), shaping how states sought to govern specifically the threat of terrorism through police and judicial cooperation (Wittendorp, 2016). The threat from terrorism was invoked in the immediate aftermath of the September 11 attacks, in 2001, and the terrorist attacks in Madrid, in March 2004, and London, in July 2005, providing once more a rationale for increased cooperation (Baker-Beall, 2016). As Bossong (2008) has explained, the 'window of opportunity' provided by the terrorist attacks, allowed the EU to push through a much wider ranging degree of broader security measures that went beyond a sole focus on counter-terrorism. Following this pattern, further counter-terrorism developments in response to the situation in Syria, have been suggested in response to the perceived terrorist threat to Europe from 'returning foreign fighters' (Bures, 2019; Baker-Beall, 2020). Throughout the history of EU counter-terrorism policy, the invoking of terrorist threats has represented a necessary precursor to continued development in this area. The arguments put forward in support of the new CT Agenda follow this pattern.

Highlighting the recent spate of terrorist attacks that took place in Europe in 2019 and 2020, the new Agenda tapped into earlier sentiments that underpinned the rationale for the development of the original EU CT Strategy, namely that terrorism represents an extreme threat to the EU and its member states. Notably however, the language selected by the EU has become increasingly more dramatic, with the idea that certain security threats, like terrorism, represent a threat to the 'European way of life' (Commission, 2020b: 2). Of course, in terms of terrorism, groups like Al-Qaida, the so-called Islamic State and other affiliates, remain a central concern. The new Agenda also singles out 'violent right and left-wing extremists' as an increasing threat. It identifies the perceived changing nature of terrorism, with a focus on lone actors that target densely crowded or highly symbolic spaces, as a new area of interest in terms of anticipatory security measures. However, it is not only known terrorist threats that are invoked by the EU as the reason for development and coordination of counter-terrorism policy.

In seeking to act preemptively to prevent terrorism from occurring in the first place, the EU has also consistently invoked the *imagined* terrorist threats of the future, which may or may not come to pass, as further justification for these developments. Nowhere is this clearer than in a report from July 2020 by the EU Counter-Terrorism Coordinator (EU CTC, Council of the EU, 2020) on the potential terrorist threats that might emerge as a result of the Covid-19

pandemic. The document is replete with reference to scenarios that *could* or *might* occur, including an increase in propaganda leading to further support for violent extremism, the enhancement (as well as potentially hampering) of terrorists' abilities to carry out attacks and an evolution towards new forms of terrorism arising from conspiracy theories that have emerged since the start of the pandemic. To provide an example of this type of thinking, one far-fetched concern involves a fear that terrorists might 'attempt to 'weaponise' the coronavirus itself to spread disease', with the claim that some 'right-wing extremists online… have discussed using Covid-19 as a bioweapon' (Council of the EU, 2020: 8-10). Importantly, these imagined threats are invoked for a particular purpose. As the document explains, the impending economic crisis in Europe, stemming from the coronavirus pandemic, will almost certainly lead to a 'reallocation of scarce budgets' and 'a smaller budget for counter-terrorism', with the CTC pointing out that not only would the 'neglect of counter-terrorism' be a 'serious mistake', but that the EU must act to 'prevent the current health and economic crisis from becoming a security crisis as well' (Ibid: 3).

The new CT Agenda builds on and appropriates these threat narratives, explaining that in order to protect citizens there is a need to better understand 'future terrorist threats'. In order to achieve this the document calls on 'foresight' to be integrated into the policy cycle, through an embrace of the insights generated from dialogue between senior counter-terrorism experts in law enforcement, intelligence and academia. For the EU, the threat from terrorism is viewed as 'real, dangerous, and, unfortunately, enduring' and, as such, requiring of renewed and sustained commitment from member states to counter the threat. Importantly, the new CT Agenda, invokes the threat from terrorism, alongside a preemptive and anticipatory security logic, for the purpose of developing a 'future-proof' environment for all of its citizens. Specifically, it is the need to better anticipate emerging terrorist threats, which provides the rationale for a 'future-proof counter-terrorism policy' (Commission, 2020b: 3). For the EU, this involves a 'whole of society' approach to security, the aim of which is to 'offer a security dividend to protect everyone in the EU' (Commission, 2020a: 3). The rationale for this approach appropriates the language of anticipatory security, noting that 'Europe needs to be more *resilient* to prevent, protect and withstand future shocks' and that this can only be achieved through building the capacity and the capability of the EU to ensure 'early detection, prevention and rapid response to crises' (Ibid. 6., emphasis added).

The EU CT Agenda and the Anticipate Workstream

The introduction of Anticipate is significant in terms of the counter-terrorism response because it reflects the move towards evermore preemptive forms of security practice and is central to the goal of developing a 'future proof' society free from dangers and threats. According to the CT Agenda, 'anticipating blind spots remain key means of strengthening Europe's counter-terrorism response and staying ahead of the curve' (Commission, 2020a: 2). Importantly, two of the key priorities outlined under Anticipate, 'strategic intelligence and threat assessment' and 'risk assessments and preparedness', remain firmly located within a precautionary approach to security. The major changes in this regard, which reflects the EU's continued commitment to preemptive security practice, concern the increased emphasis on 'reinforcing early detection capacity' through increased investment in European security research, and proposals for 'further development of new technologies' (Ibid).

In terms of reinforcing early detection, the CT Agenda highlighted two research projects, DANTE and TENSOR, that have helped to enhance the capacity of law enforcement authorities in relation to the analysis of large amounts of online data. The DANTE project

involved the creation of automated data mining and analytics solutions designed to identify and analyse terrorist related content from 'the surface, deep web and dark nets'; while the TENSOR project developed a platform for police forces to analyse large amounts of online data to help support 'the early detection of online terrorist organised activities, radicalisation and recruitment' (Commission, 2020a: 5). Similarly, further EU funded projects RED-Alert and PREVISION, have sought to develop AI capabilities for the purpose of early detection of terrorist threats and the prevention of radicalisation. Both projects involve the use of AI to support law enforcement in relation to 'more efficient and accurate processing of large amounts of data'.

With regard to the development of new technologies, the EU has proposed an important role for threat detection technologies to identify objects or substances of concern, such as bombs or bomb making materials. Here, the focus is extended beyond the aviation sector, where these types of technologies have often been applied, to railway platforms and other public spaces that it is thought might be targeted by terrorists. The CT Agenda explains that 'new technologies can contribute to the protection of public spaces if they are used in a well-defined, targeted and proportionate manner' (Commission, 2020a: 5). Specifically, the new Agenda claims that 'identification technologies capable of detecting terrorists on the move by comparing their facial image with a reference database holds security potential', while AI can play a key role in detecting terrorist threats, identifying terrorist content online and preventing its dissemination (Ibid.). The document does note a downside in that 'a key aspect to developing trustworthy AI applications is ensuring that the data used to train algorithms is relevant, verifiable, of good quality and available in high variety to minimise bias for instance towards gender or race' (Ibid.)

It is also important to note that the Respond workstream has been radically transformed and reoriented away from the logics of preparedness and emergency planning. Although the aim remains the same, to minimise the impact of a terrorist incident after it has occurred; Respond in the new CT Agenda reflects the EU move to prioritise precautionary and preemptive security measures. The new Respond workstream focuses on issues that include the strengthening of Europol and police cooperation, enhancing information exchange (including the use of the aforementioned databases like the VIS and SIS II) and support for investigation and prosecution (Commission, 2020a). Interestingly, preemptive measures targeting the financing of terrorism have been moved from Pursue to Respond in the new CT Agenda. The Commission has proposed the creation of a 'network of counter-terrorism financial investigators', for these investigators to have 'access to bank account information' and for legislation to develop 'interconnected bank account registers', all for the purpose of targeting the financing of terrorism (Ibid 20). The Terrorist Finance Tracking Programme (TFTP), including the EU-US TFTP Agreement on the exchange of financial information, is also now viewed as a key dimension of Respond.

Indeed, the measures aimed at prosecuting terrorism suspects under the Respond workstream also reflect a preemptive security approach. As with the measures that target the financing of terrorism, there is a focus on obtaining and accessing digital information that can be used to convict individuals involved in terrorism. The Commission recognises that the right to privacy should remain a fundamental principle when considering the digital communication of EU citizens but also the need for solutions to allow access for law enforcement. This includes a call for member states to work with the EU to develop protocols that can allow access to encrypted communications, the creation of an Evidence Digital Exchange System (eEDES) to facilitate cross border access to electronic evidence, and the creation of

mechanisms for the collation and sharing of 'battlefield evidence', including information uncovered and collected by military forces during battlefield operations, all as key to ensuring the successful prosecution of terrorist suspects (Ibid).

We argue therefore that the creation of the Anticipate workstream, with its focus on preemptive and precautionary security measures, and the reorientation of the Respond workstream away from the logics of preparedness, means that the EU's Counter-Terrorism Strategy/Agenda can no longer be viewed primarily as an emergency planning document. Both the EU CT Strategy and the new CT Agenda retain an approach to counter-terrorism based on the logic of anticipatory action. However, whereas the original EU CT strategy was focused on emergency planning and enhancing preparedness for terrorist attacks, with several security measures that could be described as precautionary or preemptive in orientation; the new CT Agenda focuses primarily on precautionary or preemptive approaches to security, with very little reference to the principle of preparedness. We argue that the new EU CT Agenda helps to reinforce a wider 'EU security culture' (see de Goede, 2011), which views precautionary and preemptive security as key to its development as a security actor. As such, there is an enhanced focus on preventing terrorist incidents from occurring in the first place. We now move on to consider the implications of this move to reorient EU security policy around ever more preemptive forms of security practice and, specifically, the use of new technologies to achieve a future free from terrorism.

Analysing the new CT Agenda and the Anticipate workstream

In recent decades, the use of new computer-based technologies in support of the governance of a whole range of political issues has been of increasing interest to the EU and its member states. In particular, the use of algorithms has become a perennial feature of contemporary governance, transcending Computer Science, with interest from Social Science, Law, the Humanities and so forth (Aradau and Munster, 2011; Boyd and Crawford, 2012; Kitchin, 2014; de Goede, 2012). The mass datafication of human life, combined with the prevalence of algorithms in monitoring human behaviour, has led to questions concerning blurred boundaries and debates about where 'algorithmic governance/regulation' begins and ends (Bellanova et al, 2021). The use of algorithms in health security, for example, can be traced to the 1970s and 1980s and was further propelled by the emergence of syndromic surveillance in the 1990s (Roberts, 2019). Just as the data-led, anticipatory-threat lens was pushed forward by the H1N1 virus and elevated the involvement of private corporations including Google (ibid) in the early 2000s, the Covid-19 pandemic at the start of the 2020s has re-legitimised these practices and ushered in calls for enhanced surveillance, increased monitoring and more data-driven policymaking.

Policymaking can affect the design, spread and use of algorithms, but algorithms in turn are likely to increasingly infer policymaking decisions in health, policing, trade and so forth. Given that algorithms themselves do not have pre-ordained conclusions but rather adapt to the societal-data inputs they receive, it is not so much a case of the tail-wagging-the-dog, as perhaps a mutually constitutive relationship between policymaking and data. As Roberts notes, 'algorithmic governmentality thus exhibits a new rationale of risk regulation and analysis in the digital era' (ibid:107; see also Yeung, 2018). In this context, if the EU were not actively engaging with the convergence of policymaking and algorithmic/anticipatory forms of governance, it would appear somewhat remiss.

The bloc is positioning itself as a forefront norm-creator in this arena, and we can perhaps speak of two trends. On the one hand, there is a concerted interest in nurturing an environment in which the perceived benefits of AI can be reaped. On the other hand, there is a drive to ensure that AI-facilitated governance does not encroach upon the freedoms and privacy of European citizens. These respective trends are apparent in the new CT Agenda (European Commission, 2020a: 2), the first line of which affirms that the EU 'is a unique area of freedom, security and justice, where every person must be able to trust that their freedom and security are guaranteed' and that respect for 'fundamental rights… are the foundation of our Union'. Therefore, if algorithms can foster increased security and offer material benefits to European citizens, this should be explored and exploited; with of course the caveat that in developing measures that embrace these technologies, the EU must avoid unnecessary encroachment upon the privacy of its citizens.

One of the promises of algorithmic governance is that data concerning the activities and movements of human beings across the territory of the EU can be unobtrusively used to anticipate and subsequently pre-empt or prevent terrorism. Although AI-enabled computer systems are not the only foundational block of the Anticipate pillar of the strategy, these systems are the common facilitative thread, whether the data concerns Passenger Name Record (PNR) information, financial transactions, facial recognition and so forth. It is therefore suggested by the Commission that 'Anticipation', in this context, depends upon (potentially) useful information being gleaned from a large corpus of data regarding the activities of those living within, and traveling to, the EU. The discourse in the document is more speculative than assertive; the EU is, accordingly, prepared to fund research on the best-practice utility of AI-enabled surveillance and prediction, while assessing the extent to which this activity is commensurate with fundamental EU principles. Within this light, the aforementioned DANTE and TENSOR programmes may be viewed as evolutionary steps in a broader shift towards anticipatory threat identification (Council of the EU, 2020).

This tentative approach is likely, in part, to derive from the nature of 'computer vision' itself. Computer vision in essence involves the automation of vision. A promise of computer vision is that it might enable policymakers and security practitioners – along with other stakeholders including firms – to 'see' linkages and assemblages that would not be visible through manual human-led toil. That is to say, the application of computational mathematics to collect and subsequently analyse mass data in a way that would otherwise be impossible is one avenue through which 'unknown unknowns' may be identified (Aradau and Blanke, 2015). This is emblematic of Amoore's suggestion that the 'spectre of a search for forms of calculus that open up new ways of dealing with limited or insufficient knowledge also haunts contemporary security' (2014:424). On the one hand, if a linkage of data highlights a distinct possible threat, but it is hidden away in un-mined data, the threat may remain an 'unknown unknown' and opportunities for pro-active prevention could be missed. Through data mining, it is possible that the threat could be generatively 'produced' by a computer, verified by a human being, communicated and therefore acted upon (see Amoore and Raley, 2017; Bellanova and de Goede, 2020).

On the other hand, this promise of hidden linkages has also been referred to as a 'mythology' of big data, wherein the use of computational mining applied to large datasets is believed to provide greater truths, objectiveness and accuracy than hitherto possible (Crawford and Schultz, 2013). This 'mythology' drives a desire – particularly in counter-terrorism and criminal justice efforts – to 'collect it all', which in reality may under-deliver in a context of misleading false positives and missed true positives (see for example research on the

Snowden revelations). In any case, in an anticipatory security context, if algorithms possess 'power', it emerges through this potential capacity to derive previously unforeseen linkages within mass datasets (Neyland and Möllers, 2017). The EU's speculative research into, and application of, computer vision systems, is driven by a desire to make use of practical benefits and, therefore, increased security for Member States and their citizens. Herein lies several challenges that the EU ought to seek to address when considering the applicability, utility and legality of anticipatory security through big data systems and AI.

Transparency

The first issue relates to the question of transparency. Although algorithms in various forms are today ubiquitous, certainly in well-connected and developed societies, there is a distinct difference between, for instance, the algorithms that inform Spotify's music recommendations to its userbase (Spotify, 2020) vis-à-vis pervasive state-based surveillance systems drawing on public-private partnerships. Users of Spotify's services opt-in to the surveillance of their music listening preferences. By way of contrast, the state-based mass surveillance of activities as wide-ranging as call and text records, geolocation data, transaction data – amongst others – are collected without this overt agreement. European citizens of the 21st century exist in highly developed, comparatively well-connected societies, producing voluminous amounts of data. The EU's General Data Protection Regulation (GDPR) – an international benchmark for individuals' data protection – protects the privacy of this data, although consent is not required for matters relating to national security.

There is a need to be wary of the implicit assumption that this data can and indeed should be collected and analysed because the tangible impact on the individual citizen is low, to the extent that they should not overtly notice the surveillance. In an ideal environment, the decision-making process that is sparked by algorithmic determinants would be explained to European citizens in a transparent, open manner. In practice, particularly in the case of the Anticipate pillar of the counter-terrorism strategy, this may prove problematic given the need for operational secrecy in counter-terrorism operations (Zweig, Wenzelburger and Krafft, 2018).

As Balzacq (2015) has previously argued with respect to the case of PNR-based algorithmic regulation, this is invariably a far-reaching move. With the transition towards anticipatory security practices, security is less about an environment of identified imminent threats to-be-eradicated and is instead oriented around perennial, ephemeral could-potentially-arise threats (Corry, 2012). The move to enhance security in this context serves to quieten, if not silence, public debate and scrutiny of potential encroachments upon fundamental freedoms that European citizens may have hitherto assumed they had an implicit right to enjoy. Huysmans (2016) has referred to counter-terrorism surveillance practices as 'deeply embedded' in everyday livelihoods, to the extent that routine/everyday surveillance may be regarded as a social formation that is simultaneously unavoidable and untouchable. The power imbalance within this digital data rendering (Amoore and Hall, 2009) of individuals and communities within the EU is stark. This speaks to an inherent nature of counter-terrorism bulk surveillance. Effective computer vision may depend on the greatest possible transparency with respect to its 'input' – in this case EU citizens and their data – but in the interests of promoting national security through the prevention of violent extremist behaviour, the transparency must be one-way; not bi-directional. This is emblematic of a power imbalance.

The citizenry-to-be-protected via surveillance-led practices may not – due to operational necessity – have access to specific details regarding the nature of this surveillance, but there is, nonetheless, arguably a need for transparency. The authorities in Member States may need to undertake reasonable measures to reduce discriminatory practice. As existing literature argues, claims that algorithmic-situated pre-emptive security practices are not discriminatory ought to be viewed critically (Barocas and Selbst, 2016).

Discriminatory Practices

Monahan (2018) is correct when he notes that algorithms do not function alone, and that if they are discriminatory, the 'production' and 'use' of algorithms by human beings will impact the extent to which data collection and analysis could be seen as operating in a discriminatory fashion. However, the value of algorithms derives from their capacity *to actively discriminate* on a large scale, surveying a vast quantity of data to identify correlations that may indicate potentially suspect or 'risky' behavioural patterns. The artificial intelligence element(s) of the algorithmic systems actively (re)create their profiling capacity to enhance their discriminatory accuracy. In other words, the entire purpose of algorithmic analysis of mass data – for crime fighting purposes – is to discriminate.

The CT Agenda (European Commission, 2020a) demonstrates a particular interest in precisely this AI-enabled capability. By implication, this is also an acute interest in discrimination; an anticipatory form of 'big picture' threat landscape discrimination intended to identify threats at the earliest possibility, make security-enhancing operations more efficient, and thereby enhance the security of European citizens. Note that this is not the same thing as arguing that algorithms are racist, ageist, sexist and so forth. In some cases, algorithms may inadvertently be some, or all, of these things. But it is important to recognise – and the EU discourse ought to recognise – that the value of future-facing algorithmic security derives its value from its ability to discern utility from vast amounts of data, and that this process depends on varying forms of discrimination through the computational learning of bias (Heilweil, 2020). Not all data, and therefore not all data-generators (i.e., European citizens), will be treated equally.

In the immediate present, it is likely that the issue of potential tacit discrimination by algorithmic data processing can be pragmatically side-lined, given the role played by human decision-makers, who, in the interests of effective CT operations, could potentially dismiss nefarious computer vision discrimination and instead act upon mission-critical discrimination. The existing 'intelligence dilemma' (Richards, 2012) is insufficient to hinder the practice on grounds of unfair or unethical practice. Moving forward, however, we suggest that there is a risk that once established and entrenched, AI-led surveillance *of* everyday life could in the future be combined with authentication/verification practices necessary to securely *live* that everyday life (see Muller, 2004). For instance, an individual's data presence may highlight indicators of potentially extremist behaviour, which in turn, in a future cashless era of a 'digital Euro' (European Central Bank, 2020), could lead to potential suspects being locked out of their bank accounts, able to use only a limited sum, or only able to transact in certain regions. This is not to say that such a practice is inevitable, nor do the authors suggest it would be a poor counter-terrorism approach. However, the point is that meaningful redress for errors resulting from AI-driven discrimination derived from EU-encouraged/mandated counter-terrorism operations may not be deemed necessary *now*, but will need to be implemented *before* the discrimination has a tangible impact on the livelihoods that are themselves under surveillance.

Effectiveness

Beyond the discriminatory aspects of the new CT measures envisaged under the Anticipate workstream of the new CT Agenda are important questions about the effectiveness of counter-terrorism policy. This is a perennial issue for counter-terrorism. A study by Lum et al. (2006: 8) noted that not only is there 'little scientific knowledge about the effectiveness of most counter-terrorism interventions' but that 'some evaluated interventions either didn't work or sometimes increased the likelihood of terrorism and terrorism-related harm'. These issues regarding evaluation of the effectiveness of counter-terrorism measures have also been raised with regards to the EU's own policies in this area.

A 2013 report by the authors of the SECILE project identified 88 substantive counter-terrorism measures adopted by the EU since the start of the 'fight against terrorism' in September 2001. The report found that the EU had taken very little action in the way of evaluating the impact and effectiveness of these measures. Interestingly, the report explained that as many as a third of the legally binding CT measures adopted by the EU contained no provision for review, suggesting that the EU has 'little or no concern for their impact or effectiveness' (SECILE, 2013: 17). Similarly, Leonard (2010) has noted that with regard to the EU's use of migration control measures as counter-terrorism instruments, the EU had not conducted any systematic assessment of their effectiveness in preventing terrorism from occurring.

Similar questions arise over the effectiveness of the counter-terrorism measures that are proposed under the new Anticipate workstream. Both in the EU and elsewhere, debates about the necessity for, and effectiveness of, 'collect it all' data systems that were sparked in the wake of the Snowden revelations (Crampton, 2015) are seemingly unresolved. Of particular note in relation to the 'effectiveness' of the measures implied by the Anticipate workstream are potential issues relating to the collection of *too much* data. The 'collect it all' ethos is – rationally – underpinned by the desire to ensure security by avoiding missing any data points that could lead to the successful identification of a suspected terrorist suspect. Furthermore, greater volumes of data should, in principle, improve the accuracy and capabilities of AI-facilitated data processing. Nonetheless, the contextual assemblage matters; the value of data does not merely come via more advanced computational methods. Documents from the 2013 Snowden tranche revealed MI5 memos concerning 'data overload' for operatives struggling to make effective use of the computer-derived datasets (Gallagher, 2016). This information about potential (in)effectiveness of mass data collection was – like the metadata programme itself – leaked and therefore ought not to be public-information.

These leaks indicated that the intelligence community, at least in the UK, were self-aware of the operational issues entailed by mass metadata collection. It is also possible that these may be 'teething' problems that can be ironed out with continual improvements in the technology and in the contextual assemblage. Perhaps, as the EU considers its Anticipate workstream, these issues *have* already been ironed out. The problem, from an evaluation-of-effectiveness standpoint, is that this knowledge is withheld from the public. Nor are demands for effectiveness strongly exhibited across mainstream political discourse within the EU and across Member States. As Lena Ulbricht (2018) articulated in an article on the implementation of PNR data collection, analysis and sharing in Germany in 2017, itself prompted by the EU Commission mandate, the Bill and legislative process was rushed, unopposed, and side-lined not only the implementation of effectiveness-review mechanisms

but also key elements that would be necessary to assess efficacy, including definitions, oversight and enforcement. The ephemeral, ever-prevent threat of terrorism may demand operational flexibility through legislative ambiguity, but this has important ramifications from the standpoint of transparent governance and effective security provision There is a risk that the move to data-driven anticipatory security is more symbolic than effective (Yeung, 2018).

Ultimately, given that there are questions over the effectiveness of EU counter-terrorism measures more generally, it is notable that the new CT Agenda contains no reference to the need to ascertain and evaluate the potential impact of the new measures that are being put forward as essential to the fight against terrorism.

Importance of Regulatory Oversight

The question of effectiveness links to another important issue, namely that of regulatory oversight (den Boer, 2015). The authors of the SECILE project noted in 2013 that the failure of the EU 'to properly assess the impact, legitimacy and effectiveness of its counter-terrorism policies' was odd, given the 'ample mechanisms' and 'expertise' open to the EU to conduct evaluations of EU counter-terrorism (SECILE, 2013: 28). Moreover, they suggested that the failure to utilise these resources raised issues concerning 'civil liberties and human rights, necessity and proportionality, accountability and democratic control', which speak to the 'values' often invoked by the EU when proposing new security measures. In the intervening period, since the release of the SECILE report, these concerns have not alleviated and with the focus on new computer-based methods of surveillance as important dimensions of the EU response to terrorism, issues relating to civil liberties and fundamental rights have arguably become more acute. Indeed, the advent of algorithmic governance has been likened to a form of institutional Leviathan (Konig, 2020), whereby there is a risk that, once entrenched in security practices (Brandimarte and Acquisti, 2012; Zuboff, 2019), opportunities for the EU or member states to implement a meaningful oversight regime may be missed.

Eleni Kosta's (2020) insightful article highlights how the ECtHR has already established precedent for in abstracto claims to be made in cases of mass surveillance; with 'victim' status not necessarily needing to be evidenced in relation to secret surveillance. In practice, from the perspective of the surveilled citizen, attaining and providing such evidence may be very difficult or indeed impossible. In October 2020, in a case brought by Privacy International, the Court of Justice ruled that EU member states must ensure that their legislation and practices in mass surveillance must align with the fundamental rights of European citizens. The three states in question – the UK, France and Belgium – must now return these cases to their national courts, who will be guided by the CJEU's findings (Court of Justice of the European Union, 2020). A May 2021 ruling the Grand Chamber of the ECHR found the UK's mass surveillance operations – exposed not by government transparency but instead in the 2013 leaked revelations – to have breached citizens' rights to privacy and freedom of expression (ECHR, 2021). Whilst this ruling did not establish a general legal principle *against* mass surveillance, it nonetheless bolsters the legal necessity for adequate safeguards in the 47 nation-states party to the Convention.

It could, perhaps, be argued that the European Commission is acting prematurely in its encouragement of preemptively-oriented surveillance, without necessarily having a comprehensive regulatory regime in place. Given the EU's pioneering efforts in the realm of data protection (Andrew and Baker, 2021), it would be fitting for the EU to take a similarly

norm-creating approach with respect to mediating the utility of big data systems vis-à-vis the transparency and data privacy challenges that these activities present. As noted by Murphy, with respect to EU counter-terrorism law and policy, 'if the law is ineffective, interferences with human rights are more difficult to justify and therefore more likely to be violations of those rights' (2019:222). There may not be a perfect equilibrium between developing maximum CT operational flexibility whilst avoiding unnecessarily violations of human rights, but a transparent and multi-stakeholder process could demonstrate EU and state authorities' appetite to navigate this balance.

In this light, a fully independent oversight body may be useful to ensure pro-active rather than retrospective compliance with the fundamental freedoms of the EU, as well as providing tangible assessments of efficacy which can result in recommendations and sanctions. Accountability may also come from within the algorithm-using communities themselves, in the form of whistleblowing activity from intelligence agencies, civil servants or contractors. Given that the next Edward Snowden may be a European, it is affirming to note the protections provided by Directive 2019/1937 'On the protection of persons who report breaches of Union Law', mandated to come into national legislative effect by December 2021 (European Parliament and Council, 2019).

Conclusion

In this article we have argued that EU counter-terrorism policy is increasingly focused on the anticipation and prevention of terrorist incidents before they occur. We have suggested that this reflects an emerging security culture within the EU, which views precautionary and preemptive security practice as key to its development as a security actor. The Anticipate workstream in the new CT Agenda for the EU perfectly captures this evolving ethos, with its focus on the use of new computer-based technologies as key measures in the 'fight against terrorism' and the creation of a 'future-proof society' free from terrorist threats. We have argued that although the embrace of preemptive security practices and measures - in the context of EU counter-terrorism - are not new, these developments still represent a change from initial efforts to combat terrorism at the start of the 2000s, where the focus was not only on preventing terrorism, but also on enhancing preparedness and ensuring emergency planning for the inevitable terrorist events of the future. The new CT Agenda is, by way of contrast, driven primarily by the admirable aim to pre-empt and prevent terrorism from occurring in the first place.

The new counter-terrorism measures proposed under the Anticipate workstream, designed to help achieve this aim, have been justified through the invocation of the potential terrorist threats of the future, including the threat posed by lone actors, returning foreign fighters and new forms of terrorism linked to the Covid-19 pandemic. Although on the surface these threats provide an understandable basis for the continued evolution of EU counter-terrorism policy, we have shown how they rest on a circular self-justifying logic that require anticipatory action in the present to prevent these threats regardless of the likelihood of their actualising. As such, we have argued that the embrace of anticipatory logics of security, characterised by new preemptive and precautionary security measures involving computer-based technologies as a key dimension of the response to these threats, are not without consequence.

Although it is understandable that the EU would want to explore the extent to which new technologies might be useful in supporting the response to terrorism, especially given the

ubiquity of data in present-day Europe societies; we have argued that the use of AI, algorithms or other preemptive computer-based security technologies, raises issues concerning transparency and the potential for the emergence of discriminatory practices against EU citizens. We have also identified important questions concerning the effectiveness of these measures, as well as arguing for the importance of regulatory oversight to ensure the EU lives up to its commitment to respect for the fundamental rights of EU citizens in the development and implementation of the new EU Counter-Terrorism Agenda.

References

Alexander, D. (2002). *Principles of emergency planning and management* (Oxford: Oxford University Press).

Alexander, D (2015). Disaster and Emergency Planning for Preparedness, Response, and Recovery. In: *Oxford Research Encyclopedia of Natural Hazard Science* (Oxford: Oxford University Press, 1-20.

Amoore, L. (2014). Security and the incalculable. *Security Dialogue* 45(5), 423-439.

Amoore, L. and De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change* 43(2-3), 149-173.

Amoore, L. and De Goede, M. (2012). Introduction: data and the war by other means. *Journal of Cultural Economy* 5(1), 3-8.

Amoore, L. and Hall, A. (2009). Taking people apart: digitised dissection and the body at the border. *Environment and Planning D: Society and Space* 27(3), 444-464.

Amoore, L. and Raley, R. (2017). Securing with algorithms. *Security Dialogue* 48(1), 3-10.

Argomaniz, J. (2011). *Post-9/11 European counter-terrorism politics* (London: Routledge).

Anderson, B. (2010). Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34(6), 777–798.

Andrew, J. and Baker, M. (2021). The General Data Protection Regulation in the age of surveillance capitalism. *Journal of Business Ethics* 168, 565-578.

Aradau, C. and Blanke, T. (2015). The (big) data-security assemblage: knowledge and critique. *Security Dialogue* 2(2), 1-12.

Aradau, C. and Munster, R. (2011). *Politics of catastrophe: genealogies of the unknown,* Abingdon: Routledge.

Ashley, R. (1988). Untying the sovereign state: a double reading of the anarchy problematique. *Millennium* 17(2), 227-262.

Bakker, E. (2006). Difference in terrorist threat perceptions in Europe, in: Mahncke, D. and Monar, J. (eds) *International Terrorism. A European Response to a Global Threat?* (Brussels: Peter Lang), 47–62.

Baker-Beall, C. (2013). Writing the threat of terrorism in Western Europe and the European Union: An interpretive analysis, in Bevir, M., Hall, I. and Daddow, O. (eds) *Interpreting global security* (Abingdon: Routledge).

Baker-Beall, C. (2016). *The European Union's fight against terrorism*. Manchester: Manchester University Press.

Baker-Beall, C. (2019). The threat of the 'returning foreign fighter': The securitization of EU migration and border control policy. *Security Dialogue* 50(5), 437-453.

Balzacq, T. (2015). The essence of securitisation: theory, ideal type, and a sociological science of security. *International Relations* 29(1), 103-113.

Barocas, S. and Selbst, A. (2016). Big data's disparate impact. *California Law Review* 104(3), 671-732.

Bellanova, R. et al. (2021). Toward a critique of algorithmic violence. *International Political Sociology* 15, 121-150.

Bellanova, R. and de Goede, M. (2020). The algorithmic regulation of security: an infrastructural perspective. *Regulation and Governance*, 1-17.

Bevir, M., Daddow, O. and Hall, I. (2013). Introduction: interpreting British foreign policy. *The British Journal of Politics and International Relations* 15(2), 163-174.

Bigo, D. (2008). Globalized (in)security: The field and the Ban-Opticon', in Bigo, D. and Tsoukala, A. (eds) *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (Abingdon: Routledge), 10–48.

Bossong, R., (2008). The action plan on combating terrorism: a flawed instrument of EU security governance. *Journal of Common Market Studies* 46(1), 7-48.

Bossong, R. (2012) *The evolution of EU counter-terrorism: European security policy after 9/11* (London: Routledge).

Boyd, D. and Crawford, K. (2012). Critical questions for big data: provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication and Society* 15(5), 662-679.

Brandimarte, L. and Acquisti, A. (2012). The economics of privacy. 547-571 in Peitz, M. and Waldfogel, J. (eds) *The Oxford handbook of the digital economy* (New York: Oxford University Press).

Brattberg, E. and Rhinard, M. (2012). The EU as a global counter-terrorism actor in the making. *European Security* 21(4), 557-577.

Bretherton, C. and Vogler, J. (2005). *The European Union as a global actor* (London: Routledge).

Bures, O. (2011). *EU counterterrorism policy: Terrorist threats and the European Union's responses* (London: Routledge).

Bures, O. (2020). EU's response to foreign fighters: New threat, old challenges? *Terrorism and Political Violence* 32(4), 789-806.

Corry, O. (2012). Securitisation and riskification: second-order security and the politics of climate change. *Millennium: Journal of International Studies* 40(2), 235-258.

Council of the European Union. (2005). The European Union counter-terrorism strategy. Brussels, 30 November 2005. 14469/4/05.

Council of the European Union. (2020). Terrorism in times of corona: The development of the terrorist threat as a result of the Covid-19 crisis. Brussels, 14 May 2020. 7838/1/20.

Court of Justice of the European Union. (2020). Press Release No.123/20, Judgements in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germaphone and Others. Luxembourg, 6 October.

Crampton, J. (2015). Collect it all: national security, big data and governance. *GeoJournal* 80, 519-531.

Crawford, K. and Schultz, J. (2013). Big data and due process: toward a framework to redress predictive privacy harms. *Boston College Law Review* 55(1), 93-128.

De Goede, M. (2008a). Beyond risk: Premediation and the post-9/11 security imagination. *Security Dialogue* 39(2-3), 155-176.

De Goede, M. (2008b). The politics of preemption and the war on terror in Europe. *European Journal of International Relations*, 14(1), pp.161-185.

De Goede, M. (2011). *European security culture: preemption and precaution in European security* (Amsterdam: Vossiuspers UvA).

De Goede, M. (2012). *Speculative security: The politics of pursuing terrorist monies* (Minneapolis: University of Minnesota Press).

Den Boer, M. (2015). Counter-terrorism, security and intelligence in the EU: governance challenges for collection, exchange and analysis. *Intelligence and National Security* 30(2-3), 402-419.

De Goede, M. and Simon, S. (2013). Governing future radicals in Europe. *Antipode* 45(2), 315-335.

European Central Bank. (2020). *Report on a digital euro* (Frankfurt: ECB).

European Centre for Disease Prevention and Control. (2021). Covid-19 situation update for the EU/EEA, as of 30 April 2021. https://www.ecdc.europa.eu/en/cases-2019-ncov-eueea. Accessed 1 May 2021.

European Commission. (2000). Communication from the Commission on the Precautionary Principle. Brussels, 2 February 2000. COM(2000) 1 final.

European Commission. (2004). Prevention, preparedness and response to terrorist attacks. Brussels, 20 October 2004. COM(2004) 698 final.

European Commission. (2005). Communication Concerning Terrorist Recruitment: Addressing the Factors Contributing to Violent Radicalisation. Brussels, 21 September. COM(2005)313 final.

European Commission. (2010). The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe. Brussels, 22 November 2010. COM (2010) 673 final.

European Commission. (2014). Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response. Brussels, 15 January 2014. COM(2013) 941 final.

European Commission. (2020a). EU Security Union Strategy. Brussels, 24 July 2020. COM(2020) 605 final.

European Commission. (2020b). A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Brussels, 9 December 2020. COM(2020) 795 final.

European Commission. (2020c). White paper: On artificial intelligence – a European approach to excellence and trust. Brussels, 19 February, COM(2020) 65 final.

European Commission. (2021). Eurobarometer: EU civil protection, November – December 2020.

European Council. (2003). A Secure Europe in a Better World: European Security Strategy. Brussels, 12 December.

European Court of Human Rights. (2021). *Case of Big Brother Watch and others vs. the United Kingdom*. Rome: ECHR.

European Parliament and European Council. (2019). Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law. 23 October, PE/78/2019/REV/1.

Europol. (2020). *European Union Terrorism and Situation Trend report* (The Hague: Europol).

Ewald, F. (1994). Two infinities of risk. In Brian Massumi (ed.) *The politics of everyday fear* (Minneapolis, MN: University of Minnesota Press), 221–228.

Hardy, K. (2015). Resilience in UK counter-terrorism. *Theoretical Criminology* 19(1), 77-94.

Heilweil, R. (2020). Why algorithms can be racist and sexist. *Recode*, 18 February, https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency. Accessed 1 May 2021.

Huysmans, J. (2016). Democratic curiosity in times of surveillance. *European Journal of International Security*, 1, 73-93.

Gallagher, R. (2016). Facing data deluge, secret UK spying report warned of intelligence failure. *The Intercept*, 7 June, https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/. Accessed 1 May 2021.

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* 4(1), 8-31.

Kitchin, R. (2014). Big data, new epistemologies and paradigm shifts. *Big Data and Society* 1(1), 1-12.

Konig, P. (2020). Dissecting the algorithmic Leviathan: on the socio-political anatomy of algorithmic governance. *Philosophy and Technology* 33, 467-485.

Kosta, E. (2020). Algorithmic state surveillance: challenging the notion of agency in human rights. *Regulation and Governance*, 1-13.

Larsen, H. (2002). The EU: a global military actor? *Cooperation and Conflict*, 37(3), 283–302.

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* 45(5), 494–511.

Monahan, T. (2018). Editorial: Algorithmic fetishism. *Surveillance and Society* 16(1), 1-5.

Monar, J. (2007). Common threat and common response? The European Union's counter-terrorism strategy and its problems, *Government & Opposition* 42(3), 292–313.

Monar, J. (2015). The EU as an international counter-terrorism actor: Progress and constraints. *Intelligence and National Security*, 30(2-3), 333-356.

Muller, B. (2004). (Dis)qualified bodies: securitisation, citizenship and 'identity managament'. *Citizenship Studies*, 8(3), 279-294.

Murphy, C. (2019). EU counter-terrorism law: what kind of exemplar of transnational law?. *Cambridge Yearbook of European Legal Studies* 21, 217-242.

Neyland, D. and Möllers, N. (2017). Algorithic if … then rules and the conditions and consequences of power. *Information, Communication and Society* 20(1), 45-62.

Omand, D. (2012). The terrorist threat to the UK in the post–9/11 decade. *Journal of Terrorism Research* 3(1), 6-12.

Richards, I. (2012). Intelligence dilemma? Contemporary counter-terrorism in a liberal democracy. *Intelligence and National Security*, 27(5), 761-780.

Roberts, S. (2019). Big data, algorithmic governmentality and the regulation of pandemic risk. *European Journal of Risk Regulation* 10, 94-115.

Shepherd, L. (2008). *Gender, Violence and Security: Discourse as Practice* (London: Zed Books).

Spotify. (2020). Amplifying artist input in your personalised recommendations. 2 November, https://newsroom.spotify.com/2020-11-02/amplifying-artist-input-in-your-personalized-recommendations/. Accessed 1 May 2021.

Ulbricht, K. (2018). When big data meet securitisation: algorithmic regulation with Passenger Name Records. *European Journal for Security Research* 3, 139-161.

UK Government. (2004). CONTEST: a 5-year UK strategy for countering international terrorism. Sir David Omand. Security and Intelligence Coordinator. Confidential Document. 1 April 2004.

Wittendorp, S. (2016a). Unpacking 'International Terrorism': Discourse, the European Community and counter-terrorism, 1975–86. *Journal of Common Market Studies* 54(5), 1233-1249.

Wittendorp, S. (2016b). Conducting government: Governmentality, monitoring and EU counter-terrorism, *Global Society* 30(3), 465-483.

Yeung, K. (2018). Algorithmic regulation: a critical interrogation. *Regulation and Governance* 12(4), 505-523.

Zebrowski, C. (2015). *The value of resilience: Securing life in the twenty-first century* (Abingdon: Routledge).

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for the future at the new frontier of power* (London: Profile Books).

Zweig, K., Wenzelburger, G. and Krafft, T. (2018). On chances and risks of security related algorithmic decision making systems. *European Journal for Security Research* 3, 181-203.

Zwolski, K. (2012). The EU as an international security actor after Lisbon: finally a green light for a holistic approach? *Cooperation and Conflict*, 47(1), 8-87.