Government Response to the Intelligence and Security Committee of Parliament Report 'Extreme Right-Wing Terrorism'

Presented to Parliament
by the Prime Minister
by Command of His Majesty

March 2023

CP 827

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at **publiccorrespondence@cabinetoffice.gov.uk**.

ISBN 978-1-5286-4012-1

E02887577 03/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

INTELLIGENCE AND SECURITY COMMITTEE REPORT 'EXTREME RIGHT-WING TERRORISM' GOVERNMENT RESPONSE

The Government is grateful to the Intelligence and Security Committee (ISC) for their report on Extreme Right-Wing Terrorism (ERWT). The ISC published the report on the 13th July 2022, and the then-Prime Minister acknowledged and thanked the ISC for its report in a Written Ministerial Statement on the same day.

The threat from ERWT is an important issue for the Government and we are grateful to the Committee for devoting time and attention to this subject.

The Committee began its Inquiry following the transfer of overall operational responsibility for ERWT from Counter Terrorism Policing (CTP) to the Security Service (MI5) in 2020. This occurred as a result of the Operational Improvement Review carried out in the wake of the terrorist attacks of 2017, which were the subject of separate ISC scrutiny resulting in the publication of its report entitled 'The 2017 Attacks: What Needs to Change' in November 2018. This transfer of primacy ensures a more joined-up approach to the assessment and response to both the ERWT and Islamist Terrorist threats, and allows well-established tools, practices and partnerships to be better deployed as part of the ERWT response.

The Government is committed to keeping the tools and overall strategy for tackling terrorism under periodic review to ensure that we adapt with the terrorist threat and that our response remains necessary and proportionate. In the last decade the UK has seen a range of ideologies used to justify terrorism and, in some cases, these ideologies are increasingly fragmented, with the beliefs and motivations becoming more personal. The UK must remain flexible and sufficiently agile to adapt to the terrorist threat as it evolves, reacting to whatever ideologies or narratives motivate people to become involved in terrorism. As such, our counter-terrorism strategy, CONTEST, remains threat agnostic so that rather than targeting specific ideologies, our tools, powers and overall CT approach can adapt to changing threats while also ensuring our approach is still able to identify and assess what are inherently ideological threats. On the 30th of October the Government announced that it will be carrying out a refresh of the CONTEST strategy and expects to publish this in due course.

The inquiry report does an excellent job in highlighting the range of tools needed to rise to this challenge. To achieve this, the Government is introducing new powers as part of the Online Safety Bill, and the Economic Crime and Corporate Transparency Bill such as additional tools to investigate terrorist finance, including the investigation of crypto assets. As the Committee notes in its report, there are particular difficulties in tackling terrorism and extremism online and therefore, we must work closely with partners and technology companies to ensure we have access to the tools and data necessary to better tackle these threats. For example, the recent entering into force of the UK-US Data Access Agreement will facilitate our working with content service providers based in the United States for the prevention, detection, investigation, and prosecution of serious crimes.

In producing such a comprehensive report, the Committee has continued its record of robust scrutiny of the UK's counter-terrorism system, following its previous inquiries in the aftermath of the 2013 Woolwich terrorist attack and the terrorist attacks of 2017. The recommendations and conclusions that the Committee have made following these inquiries have supported the Government's ongoing efforts to improve our response to the terrorist threat.

This document provides further detail on the Government's response to the recommendations and conclusions contained in this report. The Committee's recommendations are in **bold** below, followed immediately by the Government's reply.

A. It is clearly difficult to precisely delineate the ideologies which might motivate Extreme Right-Wing Terrorists, however we recognise that MI5 and CTP must be able to differentiate between them, not least because of the evidential thresholds.

MI5 and Counter Terrorism Policing (CTP) continue to use the Extreme Right-Wing Terrorism (ERWT) ideological categories defined by the Joint Terrorism Analysis Centre since May 2019 (White Supremacy, White Nationalism, and Cultural Nationalism) as a pragmatic way of efficiently describing the complex, shifting, and sometimes overlapping grievance narratives sitting within the ERWT thematic. However, each individual or group that they investigate is judged on the specific terrorist threat and risk they are assessed to pose, and charging decisions are the preserve of the relevant prosecuting authority, informed by evidence collected and presented by CTP.

B. Nevertheless, there is a risk that the varying terminologies used to categorise potential terrorists may cause confusion: including, most worryingly, to risk conflation of ideology with intent. It is important to be clear that there is no suggestion that all those who subscribe to these ideologies have terrorist intent, this is simply a means to establish what might be motivating potential terrorists.

In delivering its Counter-Terrorism mission, MI5 has been clear that covert investigation on the grounds of national security should be limited to those assessed to pose a threat to national security. This applies to Extreme Right-Wing Terrorism (ERWT) and other potential forms of terrorism, such as Islamist Terrorism or Northern Ireland Related Terrorism.

MI5 and Counter Terrorism Policing utilise the joint Intelligence Handling Model as a threat agnostic mechanism to assess whether an individual meets the threshold for investigation, and where it is necessary and proportionate for MI5 to take action in response to a specific national security threat.

C. More broadly, we welcome the recent addition of the word 'Extreme' to the previous term 'Right-Wing Terrorism' – it allays any possibility of the stigmatisation of those holding right wing views.

The Government welcomes the Committee's support for the addition of the word 'Extreme' to the previous term 'Right-Wing Terrorism' to distinguish these ideologies from mainstream

right-wing views. In summer 2021, the UK's Counter Terrorism System agreed to a consistent use of 'Extreme Right-Wing Terrorism' as the umbrella term for a range of ideologies and narratives, and it covers a range of ideologies and movements, including White Nationalism, White Supremacy, and Cultural Nationalism.

D. It is not surprising that there are reports that Extreme Right-Wing Terrorist groups and individuals have sought to co-opt the Covid-19 pandemic, using conspiracy theories and exploiting community grievances to attempt to radicalise, recruit and inspire plots and attacks. The full impact of the global COVID-19 pandemic has yet to be seen – but we are assured that the intelligence community and the police have recognised the impact that events such as the pandemic and the Black Lives Matter protests may have had on the extremist beliefs of individuals.

The Government welcomes this observation and agrees that this is an area of concern. The Government conducts research and analysis to maintain a contemporaneous understanding of how terrorists and extremist groups seek to radicalise, recruit and inspire attacks. This includes understanding how groups and individuals seek to exploit events like the COVID-19 pandemic or high profile protests. The resulting research and analysis plays a key role in informing the UK's operational and policy responses. We note that Lord Walney is also leading a Review on this issue and his work will be considered in due course.

Counter Terrorism Policing (CTP) and partners are alive to extremists exploiting grievances online in an attempt to radicalise and influence others. CTP work in partnership with other policing partners to assess information and intelligence in relation to groups, online fora, and individuals with an extremist ideology, and ensure their operational response is robust but proportionate. This includes joint working with front-line policing and public order policing to ensure individuals or groups who meet the terrorism threshold are investigated using all the tools available and that those who may be drawn to it are diverted away from terrorism.

E. The terrorist threat – regardless of ideology – is increasingly posed by Self-Initiated Terrorists, those who are incited or inspired rather than directed. Self-Initiated Terrorists are difficult to identify and pose a significant number of challenges in terms of detection and monitoring. Their motivation can be highly individualistic and determining how, why and when they may choose to attack is particularly difficult for MI5 and Counter Terrorism Policing. An innovative approach will be needed to counter the fragmented and complex threat posed by these disparate groups and individuals.

The UK's counter-terrorism strategy, CONTEST, is threat agnostic and is both applicable and effective in tackling various ideologies, including Extreme Right-Wing Terrorism. In addition to the ongoing threat of directed attacks from terrorist organisations based overseas targeting the UK, recent years have seen an expansion in the number of individuals, motivated by a range of ideologies, who seek to commit acts of terrorism but who are not directed or materially supported by a terrorist group. Currently, such 'Self-Initiated Terrorists', who may coordinate together independent from a wider group, and may be inspired by general directions provided by groups online, represent the dominant terrorist threat. Since 2017, three terrorist attacks in

the UK were carried out by lone actors motivated to varying degrees by extreme right-wing ideologies. These types of attack require different means to detect than larger, more complex and ambitious plots.

The 2018 version of CONTEST set out priorities for identifying and dealing with the modern threat. These included better sharing of information across government departments to support local interventions, with the legal tools and powers to disrupt threats to the UK earlier. The Counter Terrorism Operations Centre will play a critical role in responding to this changing threat. The new centre will be truly collaborative, and will unite partners from Counter Terrorism Policing, the intelligence agencies, and the criminal justice system, coordinating their expertise, resource, and intelligence, to generate a world-leading response to the threat.

There is no single pathway to becoming involved with terrorism through radicalisation, and the Government's radicalisation model applies to all forms of terrorism. The Prevent programme is fundamentally about intervening early to stop individuals from becoming terrorists, or supporting terrorism.

F. Without an agreed understanding of the links between Extreme Right-Wing Terrorism and the developmental disorders Asperger's and autism spectrum disorder (ASD) it is difficult to see how this problem can be tackled effectively. It is imperative that more is done to establish a cohesive and joined up effort across the agencies, organisations and medical professionals involved in this area.

The Government recognises the importance of close working between the Agencies and social policy departments such as the Department for Health and Social Care and the Department for Education, to improve understanding of any relationship between Terrorism and mental health and developmental disorders, including Autism Spectrum Disorders and Asperger's. There is specific work underway to build the evidence base of the prevalence and relevance of mental health and developmental disorders in counter-terrorism investigations. However, the Government remains clear that there should be no assumption that an individual who carries out a terrorist act is suffering mental ill health or has a developmental disorder, nor that someone with these characteristics is likely to carry out a terrorist act.

G. The fact that the Armed Forces do not provide clear direction to service personnel regarding membership of any organisation – let alone an extremist one – would appear to be something of an anomaly. It could be argued this is a somewhat risky approach, given the sensitive roles of many service personnel.

Whilst the Government acknowledges the concerns of the ISC when it comes to some of the sensitive roles undertaken by Service personnel, parliamentary oversight of His Majesty's Armed Forces falls to the Defence Select Committee.

The Ministry of Defence (MOD) recognises the risk of Extreme Right-Wing Terrorism within the Armed Forces and the attraction that it may offer to those who hold such views (and in particular the access to training and weapons). Extremist ideology, including but not limited to extreme right wing ideology, is completely at odds with the values of the Armed Forces and is

a matter the MOD takes extremely seriously. The MOD supports the Government's Prevent strategy and continues to work with partners across government to strengthen its internal policies and procedures for raising awareness and responding at pace when a concern is identified.

Prevention of extremism within the Armed Forces includes initial vetting on enlistment, ongoing training, raising awareness and implementing procedures to report and rehabilitate those who are at risk of being drawn into extremism. All Defence staff, including members of the Armed Forces, are prohibited from membership of proscribed organisations. Staff are permitted to join non-proscribed groups if and when it is compatible with service values and standards, in line with any individual's rights to exercise their freedom of opinion and expression.[1] This ensures that the Armed Forces are able to continue to recruit and retain personnel drawn from across society, whilst maintaining our service values and standards. Therefore, while Armed Forces personnel are permitted to join political parties and attend political meetings in a personal capacity (provided they do not wear uniform and their Service duties are not impeded), involvement in political marches or demonstrations are prohibited under the King's Regulations.

The majority of Defence personnel, including members of the Armed Forces, are subject to a level of national security vetting in accordance with Government policy, with those in particularly sensitive roles undergoing further, enhanced vetting. As part of the initial vetting process, applicants are required to self-declare associations and memberships of any groups involved in espionage, terrorism, sabotage or activities intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. In addition to this, in all recruitment applications, information provided by applicants is checked against security service records. On joining the Armed Forces, personnel receive training and instruction on the expectations of Service life, including the values and standards they are expected to uphold. This world class training, combined with the preventative measures mentioned above, help ensure that membership of extremist organisations is either minimised or identified and managed at the earliest opportunity.

H. There appears to be an issue around the current vetting processes for candidates applying to join the police – the lack of thorough background checks is a matter of concern. As the internet and the wider online sphere is the key driver of the Extreme Right-Wing Terrorism threat, it follows that online activity must be closely scrutinised when the police are assessing whether an individual is suitable to join its ranks.

The Vetting Code of Practice and Approved Professional Practice (APP) was introduced in 2017 by the College of Policing, and puts vetting on a statutory footing. Police Vetting and

---

[1] *Article 19 of the Universal Declaration of Human Rights states that 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.'*

Article 10 of the Human Rights Act 1998 states that 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'

National Security Vetting (the policy for which is owned by the Cabinet Office) are just two of a range of measures police forces test against to assess an individual's suitability to undertake a role within policing.

Police Vetting is carried out by dedicated trained staff within specialist units to ensure an assessment of any potential risk is conducted in relation to those working for, on behalf of or alongside the police. It includes checks on local and national force systems, open-source social media profiles, associations of the individual, and financial checks. The extent of these checks depends on the level of vetting that is required for the individual's job role. The APP is regularly refreshed and amended to ensure it takes regard of emerging risks, threats, or changes in legislation, as well as learning from cases or inquiries. This would include checking for indication of Extreme Right Wing affiliations, as well as other extremist ideologies considered incompatible with serving as a police officer. Membership of a proscribed organisation or other group or association that has aims and objectives that are contrary to the Code of Ethics and standards of professional behaviour will ordinarily result in vetting clearance being withheld.

All police officers and staff are subject to a renewal of their vetting. The different levels of vetting have different timeframes for renewal that range from three to ten years. For the higher levels of vetting, checks are completed annually to assess suitability to continue to hold vetting clearance. Vetting is only a snapshot in time, and in the time between clearance being granted and the full re-vetting application, officers and staff are obliged to notify their vetting unit of any changes to their circumstances. The vetting status of an individual is also reviewed if they are subject to a misconduct finding or criminal investigation once it has concluded.

In conjunction with the College of Policing, the National Police Chiefs Council vetting portfolio is undertaking work to ensure that the measures that vetting practitioners are currently taking are sufficiently robust and looking at technological solutions to assist with the emerging risk around social media and open-source footprints.

I. There is no process in place to monitor those 'G*' individuals who have travelled overseas for Extreme Right-Wing Terrorism-related purposes and have returned to the UK – there is a strong possibility that these returning foreign fighters, some of whom may have fought ***, will have been further radicalised ***, and developed connections with others who share their Extreme Right-Wing ideology.**

We recognise the risk factors outlined by the Committee. MI5 and Counter Terrorism Policing, in line with their joint Intelligence Handling Model, judge the appropriate action to take on a case-by-case basis, depending on the understanding of the specific risk posed. This could include covert investigation, criminal arrest, or direct engagement with the individual, depending on the circumstances.

Anyone who travels to a conflict zone, having gone to support a proscribed organisation or for other illegal purposes, can and will be investigated by the police. Any investigation is carried out with an open mind and based on the evidence available. This is to determine if individuals have committed any terrorist or other criminal offences, regardless of their motivation, and to

ensure they do not pose a danger to the public or to UK national security. Any decision to bring charges against an individual ultimately rests with the relevant prosecuting authority.

J. The Mixed Martial Arts (MMA) are a popular activity enjoyed by many people across the UK. The fact that this is an area which is currently being targeted by the Far Right in other countries, and that a number of MMA instructors were previously have been found to be involved in National Action, suggests that MI5 and Counter Terrorism Policing should be alert to the potential for links in the future.

As the Committee highlights, Mixed Martial Arts (MMA) is a mainstream sport enjoyed by large numbers of participants and spectators across the UK, the vast majority of whom are not engaged in any activity of UK national security concern.

The Government thanks the Committee for flagging the potential for targeting of MMA by Extreme Right-Wing Terrorist actors and will continue to be mindful of such links in future. In line with MI5 and Counter Terrorism Policing's joint Intelligence Handling Model, judgements on appropriate actions to take are made on a case-by-case basis, depending on the understanding of the specific risk posed by the individual or group in question.

K. Nevertheless, it is clear that the Extreme Right-Wing Terrorism online environment poses a new challenge for the intelligence community, and there is still a long way to go when it comes to tackling what is largely an ungoverned space. The Head of Counter Terrorism Policing told the Committee that "*the single biggest thing that keeps me awake at night is the proliferation of online [sic] and its ability to radicalise and incite people*." Director General MI5 pointed to the particular challenge of determining Extreme Right-Wing activity online which could translate into 'real-world' terrorist activity:

> ***the activity itself is often just online espousal of violent views without any real world accompanying activity and so often we are monitoring something which is just online and nothing else, potentially for years on end, but it doesn't take much for an individual or a small group of individuals to change their direction and do something violent in the real world.***

The Government is aware that the Committee has long held an interest in this area and has contributed to considerations of how we counter terrorist activity online. As the Committee's report notes, the landscape has grown more complicated, including increased and changing Subject Of Interest behaviour, and availability of different services and platforms. The high level of rhetoric which characterises the Extreme Right-Wing Terrorism (ERWT) online environment, not all of which translates into actual activity of national security concern, poses a considerable challenge for MI5 to identify and prioritise those individuals who will actually mobilise to become involved in terrorism. This challenge is compounded by the radicalising and incitement potential of the proliferation of ERWT material in the online space.

The Government is deploying the very best of its 'Preventing Terrorist Use of the Internet' approach to tackle all forms of terrorism online, including ERWT. We are leveraging our

relationships with technology companies, international partners, and civil society, to reduce the risk of radicalisation and disrupt ERWT content and activity online. We are working across Government and with our stakeholders to coordinate efforts and to hold technology companies to account.

In 2010, the Government set up the Counter Terrorism Internet Referral Unit (CTIRU), based in the Metropolitan Police. The CTIRU identifies, assesses and refers online content that is in breach of UK terrorism legislation to technology companies for removal, in accordance with platforms' terms and conditions. To date, over 314,500 individual pieces of terrorist content referred by CTIRU have been removed by companies. However, the Government has been clear that technology companies cannot be reliant on law enforcement referrals – they need to work together and act more quickly to remove all forms of terrorist content from their platforms.

The Government has also published its Online Safety Bill – a truly world-leading and much-needed law that will make the UK the safest place to be online. The Online Safety Bill will give effect to a new regulatory framework; for the first time, technology companies will be accountable to an independent regulator to keep their users safe. Companies will need to remove and limit the spread of illegal content, and clearly set out and consistently enforce their terms and conditions.

We continue to focus on ERWT online issues as a priority alongside other online threats such as Islamist Terrorism, and judge that the majority of ERWT activity of concern (short of actual terrorist attacks) is likely to occur online in the years to come.

L. The Operational Improvement Review and its practical recommendations signalled a fundamental shift in the Government's approach to what was then termed 'Domestic Extremism' – the subsequent transfer of lead responsibility from Counter Terrorism Policing to MI5 regarding what was by then recognised as a terrorist threat was a pragmatic and logical move.

MI5 took full intelligence primacy from Counter Terrorism Policing (CTP) in April 2020, going further than recommended initially in the Operational Improvement Review. The move to bring Extreme Right-Wing Terrorism (ERWT) into alignment with Islamist Terrorism has enabled the UK Intelligence Community and CTP to bring to ERWT the same partnerships and approach to countering terrorist activity that has been used against the Islamist Terrorist threat for some years. This model will evolve and improve as the community delivers its counter-terrorism mission going forward.

M. The continuing rise in the number of referrals to Prevent for concerns around Extreme Right-Wing activity does not necessarily signal a similar increase in the Extreme Right-Wing Terrorism threat, but rather indicates a greater awareness of the potential risk and the greater focus being placed on this issue. We consider that the Home Affairs Committee may wish to examine how and why people are being referred to Prevent – and who is making these referrals.

An Independent Review of Prevent has now concluded and was laid in Parliament on Wednesday 8 February 2023, alongside the Government's response to the 34 recommendations made by the Reviewer. This will ensure that we continue to improve our response to stop people from becoming terrorists or supporting terrorism. This is part of an ongoing Government commitment to ensuring the Prevent programme is as effective as possible, and is able to intervene early to divert people away from radicalising influences from across the spectrum of extremism, including those inspired by the Extreme Right-Wing. It should be noted that the Reviewer made particular reference to the need to ensure that Prevent works to a consistent and proportionate threshold across all extremist ideologies, in order that Prevent remains focussed on its objectives and does not capture mainstream politicians, commentators or publications.

Prevent referrals are just one metric that we use for monitoring risk and threat. The Home Office and Counter-Terrorism Policing take into account a variety of other indicators to assess levels of threat across ideology types, such as community sentiment, the conversion of referrals to adopted Channel cases, and intelligence assessments from our security partners. An increase in Prevent referrals can be used as an indicator of the prevalence of radicalisation concerns, but it is important to avoid asserting that an increase in referrals directly correlates to in an increase in risk. In some cases, an increase in Prevent referrals can indicate an improved understanding and awareness amongst practitioners, due to undertaking training or closer partnership working. Following the Independent Review, Prevent will introduce a new security threat check process to underpin decision-making at a strategic level. This will give partners and the wider public further reassurance about the rationale behind Prevent decision-making and ensure it is proportionate and consistent with the threat we face.

N. Advocacy groups can play an important role, however we recognise that MI5 and Counter Terrorism Policing may be constrained in the way in which they are able to interact with them at an operational level, and would encourage the Home Office to develop constructive relationships at a strategic level instead.

The Prevent strategy, which works to stop people becoming terrorists or supporting terrorism, engages closely with the charity and voluntary sectors to ensure that they have the understanding and awareness they need to identify those at risk of radicalisation and refer them to Prevent when appropriate.

Prevent also works closely with civil society organisations to deliver counter radicalisation initiatives within communities, including groups with a specific expertise in Extreme Right-Wing Terrorism (ERWT). This includes delivery of community projects to counter specific ERWT threats and a programme of capability activity to upskill organisations, share best practice and develop successful interventions.

In addition, Prevent engages with relevant advocacy groups (interest groups concerned with advocating for change in particular areas of policy) at a strategic level to broaden our sources of insight and help us to better understand and analyse the problem of extremism and radicalisation.

O. MI5 have taken on responsibility for Extreme Right-Wing Terrorism (ERWT) without the commensurate resources. Taking the month of July 2020 as an example, ERWT and Left, Anarchist, Single-Issue Terrorism (LASIT) casework accounted for around under a fifth of all Counter Terrorism investigations: that casework can only be undertaken at the expense of other MI5 work. The impact has been seen on * casework, which is now progressed more slowly, and on MI5's inability to expand its work on other threat areas, as it had intended. This situation is untenable. While MI5, rightly, allocates its resources on what it assesses to be the highest priority work based on its expert knowledge of the threat, we are concerned that they have been expected simply to absorb this new responsibility. MI5 must be given additional funding to enable it to conduct these cases without other areas of work suffering as a consequence.**

The latest Spending Review settlement, agreed in 2021, provides the Single Intelligence Account with a £0.7 billion cash increase over three years to £3.7 billion in 2024-25. This supports delivery of the priorities set out in the Integrated Review and will ensure the UK's Intelligence Community can continue to retain their world-leading capabilities to counter national security threats to the UK. The settlement supports the delivery of the world-leading Counter Terrorism Operations Centre which co-locates the UK Intelligence Community, Counter Terrorism Policing, and other parts of the criminal justice system.

MI5 deploys its investigative, analytical and operational resources flexibly across all areas of national security threat in response to demand. MI5's balance of effort will therefore flex over time in response to this picture. This balance is kept under constant review by the MI5 Executive Team. As the Committee highlights, MI5 is operationally independent in terms of the decisions it takes in prioritising threats to national security, aligned with the terms of strategic direction to Government priorities as set in the Integrated Review and by the National Security Council.

P. It is clear that the Behavioural Science Unit (BSU) is making a vital contribution to promoting an informed understanding of the complexities of the Extreme Right-Wing Terrorism (ERWT) threat. We are puzzled that MI5 does not appear to be taking active steps to ensure it has the capacity to be involved at the outset of all investigations. The BSU is clearly an essential capability, particularly when it comes to meeting the ERWT threat, and must be resourced appropriately.

The assistance provided by the Behavioural Science Unit (BSU) is one of a range of tools available to all MI5 investigators and operational teams, where and when appropriate.

The BSU meets, as a matter of course, all analysts, investigators and operational staff to discuss the support and expertise available in the BSU for ERWT-related casework. There are well-used and familiar mechanisms for people working across MI5 to access that deep level of thematic ideological expertise as necessary.

Q. Proscription has, to date, been an important disruptive tool in countering the influence and activities of bodies and organisations which seek to carry out terrorist activity. However, the ideologies driving Extreme Right-Wing Terrorism are complex, and in the

case of, for example, neo-Nazi groups such as Order of Nine Angles, do not meet the terrorism threshold. We note that Counter Terrorism Policing and the Home Office are considering a possible review of the current proscription process – this is a welcome development.

The Government recognises that it is important to keep the effectiveness of the counter-terrorism toolkit, including proscription, under continual review to ensure that it keeps pace with the evolving, modern terrorist threat. During its Inquiry, the Committee heard evidence from the Government and operational partners confirming that proscription remains an important disruptive tool; one that has been used successfully against Extreme Right-Wing Terrorist (ERWT) organisations.

Five ERWT organisations have been proscribed since December 2016, and several aliases of these organisations recognised. Proscription has been used to successfully disrupt National Action, which began as a traditional street-based organisation, and it has also been used against organisations that exist almost exclusively or wholly online with members from across the world. The Government is aware that UK-based individuals are becoming increasingly cognizant of the risks associated with online ERWT groups and as a result, some are being deterred from joining them. The impact of proscription is kept under regular review. This includes analysis from the Independent Reviewer of Terrorism Legislation, who has privileged access to decision making relating to proscription, liaison with international partners, and classified internal evaluation that examines the outputs and outcomes associated with proscription.

Continual review of the counter-terrorism toolkit remains crucial as the threat from online spaces continues to grow, and these groups transition from organisations with clear structures and leadership to loose collections of individuals occupying various extremist eco-systems online.

R. The Government will need a new approach to tackle the financing of Extreme Right-Wing Terrorism (ERWT). It is one thing to take an agnostic approach and shared methodology in assessing the Islamist terror threat and ERWT, however when it comes to the financing of this activity the reality is that the two are very different. Moreover whilst it would appear that at present the financing of ERWT is low-level and ad-hoc, the reality is that this could change rapidly as the threat evolves.

As part of the Government's work to detect, prevent, deter and disrupt the flow of Extreme Right-Wing Terrorist (ERWT) financing, the Home Office continues to engage and collaborate with wider stakeholders including law enforcement, the financial sector, and non-Government organisations. The Government recognises, in particular, that financial intelligence, including through terrorist-related financial transactions, continues to be a hugely valuable tool to investigations, allowing operational partners to develop a comprehensive understanding of a suspect's lifestyle, spending activities and associations, which in turn can lead to further investigative enquiries to uncover and exploit wider ERWT networks.

The Government already has plans in place to update the counter-terrorism legislation through the Economic Crime and Corporate Transparency Bill later this year, to ensure that our robust legislation keeps pace with emerging threats and technologies such as crypto-assets. We will continue to take a proactive approach to emerging threats and trends to ensure we have the tools and capabilities to manage them, and by providing our law enforcers with wide-ranging legal powers to disrupt and pursue terrorist financing.

S. It appears that there are inherent difficulties with these voluntary Codes of Practice, and indeed across the Online Safety Bill more widely. Whilst the major communication service providers – who are already on board with the government's drive to promote responsible behaviour – are adhering to these principles, it is the smaller organisations (many of which are particularly influential in the Extreme Right-Wing Terrorism space) who appear reluctant to step up. The emergence of many 'free speech' unmoderated platforms specifically aimed at the Extreme Right-Wing are also a problem. It will be essential for Ofcom to develop the expertise and technical know-how as a matter of urgency if they are to be able to properly enforce mandatory codes of practice across the industry.

The Government welcomes the Committee's interest in this important issue. Under the Online Safety Bill tech companies will be accountable to an independent regulator (Ofcom) to keep their users safe. Platforms that fail to protect their users will need to answer to the regulator. Ofcom will have robust powers to take enforcement action against companies who do not comply with their new duties and protect users from harm. These powers include imposing substantial fines of up to £18m or 10% of global revenue (whichever is higher), requiring companies to make improvements and applying for business disruption measures, including blocking, via the courts.

The introduction of the Bill should be taken as a clear message to companies that they need to begin preparing for regulation now. The Government expects companies to take steps now to improve safety, and not wait for the legislation to come into force before acting.

Ofcom has experience taking on and delivering a breadth of complex high-profile remits and taking a risk-based and research-led approach to regulation. It is experienced at dealing with a high volume of small businesses. Since November 2020, Ofcom has been the regulator of popular video-sharing services including Vimeo, Twitch, Snapchat and TikTok. This video-sharing platform regime allows Ofcom to test and formulate its regulatory processes ahead of the commencement of the Online Safety framework. Once the Online Safety regime is operational, this will be repealed. Further guidance on the video-sharing platform can be found on the Ofcom website.

The Government is working closely with Ofcom to identify how it can continue to build the full range of necessary capabilities, including technical expertise. Ofcom is actively strengthening its digital capabilities, including recruitment of experts from the private sector, international organisations, and civil society. These capabilities are dedicated to illegal activities related to hate and terrorism with a focus on the platforms that are conductive to

hosting them. Ofcom are building their knowledge base through research partnerships that focus on UK specific prevalence.

Ofcom will also build strong working relationships with law enforcement to deliver a coherent approach to tackling online harms, including how their responsibility to regulate systems and processes interacts with law enforcement responsibilities to investigate illegal activity. They are already in the process of working with the UK's intelligence community and law enforcement to build an understanding of roles and responsibilities, lessons on engaging with online platforms and to share information on safety technologies that support the effective detections and removal of illegal content.

T. International co-operation is key to tackling Extreme Right-Wing Terrorism, however the disparity in approach and legal thresholds for defining the threat makes this particularly challenging. MI5 and Counter Terrorism Policing are committed to exploring a possible joint approach with international liaison partners, although we note that the nature of the problem varies greatly across different countries.

The Government agrees with the Committee that international co-operation is important to tackling the threat from Extreme Right-Wing Terrorism (ERWT), as it is with the full range of covert threats to national security that MI5 confronts. Given the differing nature of the threat, thresholds for action, and legal positions found in each country, efforts have focused on mutual learning and sharing best practice.

MI5 also collaborates bilaterally with international partners on a tactical basis as casework dictates. These international partnerships have allowed MI5 to come to grips with the ERWT threat in the UK at a faster pace, facilitating learning from other best practices and checking thinking against a wider evidence base. MI5 remains focused on continuing to develop its bilateral and multilateral engagement on ERWT.

U. It is encouraging that the strong operational relationships built up over the years by the intelligence community and police with their European counterparts continue to develop in the post-Brexit era. Whilst most capacity has not been affected, we remain concerned about possible loss of access to some important capabilities, such as Passenger Names Records. We emphasise the need for ongoing discussion on alternative arrangements to succeed.

As part of the Trade and Cooperation Agreement with the EU, the Government maintained the transfer of EU Passenger Name Record (PNR) data to the UK and retained the capability to process and use the data for the purposes of preventing, detecting, investigating or prosecuting terrorism or serious crime. Additionally, the agreement with the EU extended the purposes for which PNR data may be used by the UK to include, in exceptional cases, protecting the vital interests of individuals at risk of death or serious injury, or from a significant public health risk. These additional purposes are outside of the scope of the EU PNR Directive which guides the use of PNR data by EU Member States.

INTERPOL allows us to exchange information with EU Member States on persons of interest, including missing and wanted, and on lost and stolen documents. All incoming INTERPOL circulations (notices and diffusions) are uploaded to UK border and policing systems. Whenever a check is made on those domestic systems, international circulations are simultaneously checked. Our use of INTERPOL provides the capability to exchange data and communicate with all our international partners quickly and securely. The UK has an excellent relationship with INTERPOL which has developed considerably in the last three years. We continue to provide and expand our support for the institution through funding, expertise, and data. The International Law Enforcement Alerts Platform (I-LEAP) is a new capability that will provide real-time access to data and facial images of INTERPOL nominal (persons of interest) and objects to front line UK law enforcement and UK border officers. In the longer term, I-LEAP will enable reciprocal alert exchange with key international partners.

E02887577

978-1-5286-4012-1