RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

DEMOS

Occasional Paper

The Personal Security of Individuals in British Public Life

Alexander Babuta and Alex Krasodomski-Jones

The Personal Security of Individuals in British Public Life

Alexander Babuta and Alex Krasodomski-Jones

RUSI Occasional Paper, June 2018

Royal United Services Institute
for Defence and Security Studies

187 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 187 years.

About Demos

As the UK's leading cross-party think tank, Demos is a champion of people, ideas and democracy. For 25 years Demos has looked to bring people together, to bridge divides and to listen. Demos's four research programmes cover issues of UK social policy, the modern economy, international social and cultural issues, and how the rise of the digital world affects politics, policy and decision-making.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2018 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, June 2018. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The authors are very grateful to a number of individuals who provided valuable feedback and comments on an earlier version of this paper, particularly Professor Malcolm Chalmers, Dr Andrew Glazzard, Dr David James, Dr Paul Martin and Professor Alison Wakefield. The authors would also like to thank the RUSI publications team for their expert editorial input in producing the report, particularly Dr Emma De Angelis, Zenab Hotelwala, Sarah Hudson, Edward Mortimer and Stephen Reimer.

Executive Summary

- There is a wide spectrum of threats facing individuals in British public life, most of which result in psychological rather than physical harm. At the less severe end of the spectrum, it is often difficult to discern where the boundaries lie between legal and illegal behaviour.
- While many threats affect private citizens as well as individuals in public life, threats directed at public figures have a wider cumulative impact on societal stability, and may undermine the democratic process.
- There is a broad range of perpetrators responsible for threats to public figures, ranging from casual 'trolls' through to coordinated agents of hostile states seeking to cause damage to a government or society at large.
- Malicious communications rarely develop into direct threats to an individual's physical safety. However, the most severe physical threats are typically preceded by a range of precursor activities, including harassment, stalking and other fixation-related behaviour.
- Official responses to the security threats facing individuals in public life have so far been varied and uncoordinated. There remains disagreement and misunderstanding over governance arrangements, duties of care and accountability.
- Close protection is only offered to a very small number of high-profile individuals in Britain, and there is a large 'middle ground' of individuals in public life, including most politicians, who are undoubtedly at a higher risk than general members of the public, but receive only minimal support.
- While it appears that threats to public figures from social media have grown in recent years, systematic evidence on this phenomenon is lacking, and the true scale of online threats to public figures is at present poorly understood.
- There remains disagreement over the most appropriate response to the problem of online abuse, particularly in terms of the roles and responsibilities of social media companies. Treating technology companies as publishers (rather than platform hosts) has frequently been proposed as a potential solution, but this would be problematic and complex to implement in practice.
- While social media companies may be better placed than law enforcement to detect online activity related to stalking and attack planning, questions remain over the responsibilities and jurisdictions of technology companies in fighting crime.
- A multi-agency approach, based on a clear division of responsibilities and which engages a range of stakeholders, is likely to be the most effective response to threats facing individuals in public life.
- Research shows a very high prevalence of mental illness among those who commit or attempt to commit criminal attacks against public figures. The role of psychiatric intervention is therefore particularly relevant for prevention. A public-health approach has been effective in reducing violent crime, and population-wide psychiatric

interventions may similarly reduce the risk to public figures by reducing overall risk of violent criminality linked to mental illness.

- The Fixated Threat Assessment Centre (FTAC) is one example of a successful multi-agency initiative that has since been replicated overseas, involving police officers working closely with forensic nurses, social workers, forensic psychiatrists, and psychologists.
- While some have called for new legislation to address threats to public figures emanating from the online space, all evidence suggests that existing legislation is sufficient to prosecute for criminal offences committed against individuals in public life, both online and offline.
- In order for legislation to be effective, it relies upon consistent reporting by victims, and better understanding throughout the criminal justice system about stalking and abuse. Lack of reporting by victims and poor understanding of the threats both remain significant barriers to progress.

Introduction

THIS OCCASIONAL PAPER explores the personal security of individuals in British public life. Much of the content is based on the proceedings of a half-day conference held at the Royal United Services Institute (RUSI) on 23 January 2018, organised in partnership with Demos and made possible with the generous support of the Airey Neave Trust and SEAK Global.[1] Attendees included Members of the House of Commons and House of Lords, academics, legal experts, current and former government practitioners and policymakers, law enforcement representatives, representatives from the private sector, NGOs, and individuals with direct personal experience of abuse, harassment and stalking.

This paper focuses specifically on the threats faced by British politicians and those who are employed by the state. While it may be difficult to generalise, previous research has found that the issues discussed in this paper manifest themselves in much the same way in other countries such as Australia, New Zealand and Norway.[2] Additionally, these problems have existed in some form for many decades, though recent years have seen the threats manifested in different ways, driven primarily by developments in technology and in particular the growth of social media.

The paper seeks to first define the problem through characterising the spectrum of threats, the range of perpetrators and of potential victims before discussing potential responses and the division of responsibilities for delivery of protective services.

[1] The Airey Neave Trust identifies and supports selective publications and seminars on current and potential anti-terrorist issues. See <http://www.aireyneavetrust.org.uk/>. SEAK Global is a specialist provider of personal safety, crisis and security risk management technology. See <https://www.seakglobal.com/>.

[2] The prevalence of gun ownership in the United States makes the situation there considerably different. See, for example, David V James et al., 'Aggressive/Intrusive Behaviours, Harassment and Stalking of Members of the United Kingdom Parliament: A Prevalence Study and Cross-National Comparison', *Journal of Forensic Psychiatry and Psychology* (Vol. 27, No. 2, 2016).

I. Defining the Problem

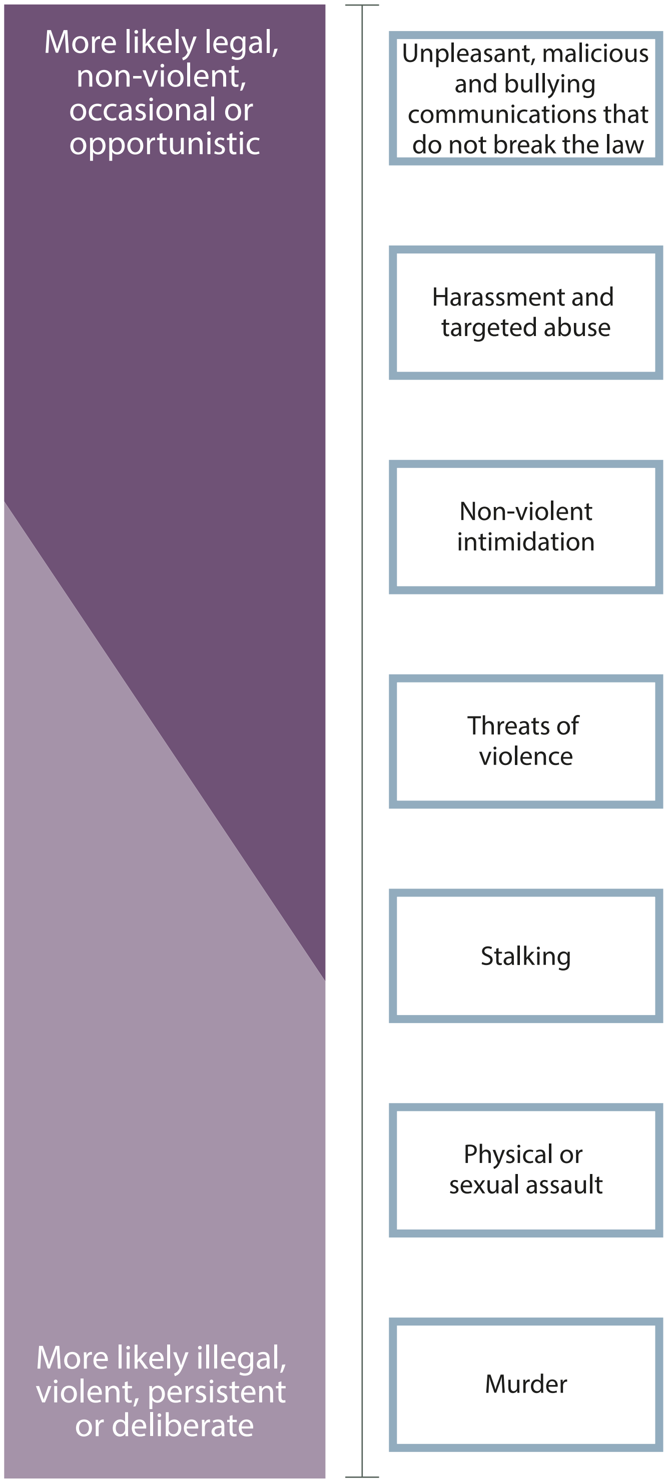
Threats

INDIVIDUALS IN PUBLIC life face a diverse range of potential threats from numerous sources with different potential causes and consequences. Threats can range from bullying (both in person and through malicious communications), persistent abuse and harassment, intimidation, stalking, and threats of violence to individuals, their families and staff to the most serious criminal offences, including physical or sexual abuse, assault, and, in a number of tragic cases, murder.

In this paper, 'public figures' refers to any individual with a prominent public or media profile. This includes celebrities, media personalities, journalists, members of the royal family, politicians, high-profile businesspeople, and other high net-worth individuals. The focus of this paper is specifically on politicians and those who are employed by the state. While other public figures also suffer much of the same problems as politicians and government employees, the protection arrangements for celebrities and private sector employees are very different. Many of the issues discussed in this paper may also apply to the private security sector, but that is not the focus of this paper.

Based on a review of the literature outlined in this paper, as well as the issues discussed at the RUSI conference, the authors understand the threats facing public figures to sit on a spectrum (Figure 1), loosely linked to how severe a threat they pose. Of course, individuals who are not in public life are also targeted by such behaviour. However, when these threats are directed at public figures they can undermine the democratic process and have a wider detrimental impact on societal stability and security.

Figure 1: Spectrum of Threats Faced by Individuals in Public Life


More likely legal, non-violent, occasional or opportunistic
More likely illegal, violent, persistent or deliberate
Unpleasant, malicious and bullying communications that do not break the law
Harassment and targeted abuse
Non-violent intimidation
Threats of violence
Stalking
Physical or sexual assault
Murder

Source: The Authors.

One of the main difficulties in characterising these threats at the less violent end of the spectrum is that there is subjectivity involved when assessing what constitutes abusive behaviour, and limited legal protection from communications or actions that may be upsetting, but are not necessarily illegal. The majority of the threats outlined above result in psychological rather than physical harm, and it is often difficult to discern where the boundaries are drawn between legal and illegal behaviour. In the majority of cases where individuals have come to serious physical harm, the ultimate criminal act has been preceded by a range of precursor activities, typically including harassment, stalking and other fixation-related 'warning behaviours'.[3] For instance, a 2017 study examining 358 cases of criminal homicide against women in the UK over a three-year period found that stalking behaviour was present in 94% of the cases, with threats to kill in 55% of cases.[4] This has significant implications for prevention and disruption, as there are often numerous opportunities for potential victims to spot the early warning signs that they are being targeted by such behaviour, and for the authorities to investigate and prevent any further harm.

In many cases these threats also include aspects of discrimination. Abuse specifically targeted towards women, particular ethnic groups or other minorities, may fall within the scope of hate crime legislation, adding an extra dimension of severity beyond casual 'trolling' and bullying. The discriminatory component of this behaviour should then be considered as an aggravating factor if it is assessed that an offence has been committed.

The threats are each associated with different types of harm, of varying severity. At the less severe end of the spectrum, psychological distress and offence caused to individuals and those around them is the most common form of harm. When malicious communications involve intimidation and threats of violence, this often causes individuals to fear for their own physical security and that of those around them, which may lead them to change their behaviour and routines. There is also the risk of escalation from non-violent intimidation to more serious forms of behaviour. For public figures, these threats also have the potential to cause public embarrassment and defamation, and risk disrupting their official public functions and hindering their capacity to effectively do their job.

When threats to public figures are severe enough to impede their ability to effectively carry out their public functions, this results in a number of second-order effects. Threats tend to be viewed through the lens of harm done to an individual: this is reflected in everything from the legal system to popular perceptions of how harmful any given behaviour might be. However, it is important not to overlook the cumulative effect of persistent and pervasive threats that might in isolation be discounted, but over time have a degrading impact on the very fabric of

[3] David V James et al., 'The Role of Mental Disorder in Attacks on European Politicians 1990–2004', *Acta Psychiatrica Scandinavica* (Vol. 116, No. 5, 2007); J Reid Meloy et al., 'The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology', *Behavioral Sciences and the Law* (Vol. 30, No. 3, May/June 2012).

[4] Jane Monckton-Smith, Karolina Szymanska and Sue Haile, 'Exploring the Relationship Between Stalking and Homicide', Homicide Research Group, University of Gloucestershire Centre for Learning and Innovation in Public Protection, Suzy Lamplugh Trust, 2017.

politics and society. Whether messages on social media, headlines in national newspapers or anger on the streets, threats which in isolation may not appear particularly severe often cause wider harm to society and democracy, and this must be taken into account when considering potential responses.

Perpetrators

The threat actors responsible for such activity are many and varied: political activists and protestors seeking to push the boundaries of offensiveness and expose hypocrisy through online 'trolling';[5] irate or disgruntled members of the public venting their personal frustration to members of the 'establishment' or political elite; mentally ill and fixated individuals who become obsessed with certain public figures; political and ideological extremists who wish to further a particular cause; or – at the more organised end of the spectrum – agents of hostile states seeking to undermine democratic processes and weaken state institutions. In the case of online abuse, definitions have become blurred, with 'trolling' used to describe everything from satirical and offensive provocations to the most serious threats of violence. While this malicious activity is typically focused on particular individuals, as noted above it has a broader cumulative impact on societal stability, and can therefore be used as a tool by politically motivated individuals or groups seeking to cause damage to a government or society at large. In recent years, the integrity of the democratic process in the UK has no doubt been undermined by persistent abuse and intimidation directed towards parliamentarians and ministers, along with reported attempts to wage industrial-scale information warfare campaigns by hostile foreign states.[6]

Both online and offline, the past five years have seen an increase in the number of parliamentarians reporting a sense of being under threat.[7] In the period leading up to the EU referendum, Demos research found upwards of 80,000 abusive messages directed towards parliamentarians on one social media platform alone.[8] Although digital channels have offered a new way for politicians to interact with their constituents and the electorate, they have also left them more vulnerable to abuse, intimidation and harassment.[9] Parliamentarians are uniquely vulnerable to threats

[5] Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (London: William Heinemann, 2014), pp. 13–46.

[6] Committee on Foreign Relations, United States Senate, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security', 115th Congress, Second Session, 10 January 2018.

[7] Committee on Standards in Public Life, *Intimidation in Public Life: A Review by the Committee on Standards in Public Life*, Cm 9543 (London: The Stationery Office, December 2017).

[8] Alex Krasodomski-Jones, 'Signal and Noise: Can Technology Provide a Window into the New World of Digital Politics in the UK?', Demos, May 2017.

[9] The impact of online channels on the levels and styles of communication is beyond the scope of this paper. Online anonymity, disinhibition effects and a lack of existent standards of behaviour or communication are often cited as reasons for a lower quality of discourse online as compared to offline.

from the public, as their roles require them to operate in the public domain, including online. They are also required to provide specific times and locations for their availability for personal meetings with constituents, making them vulnerable to threat actors of all types.

Against this background noise of digital abuse, research shows that the primary threat to the safety of elected politicians in Western countries comes not from terrorist groups, but from ‘fixated loners’.[10] The risks posed by such individuals extend far beyond physical violence, and include unwanted communications, unwelcome contact and other associated ‘fixation’ behaviours. Direct hostile action is typically preceded by a series of warning signs or ‘leakage’ in the form of abusive or intrusive communications. Fixated individuals – in contrast to most internet trolls – typically make themselves personally known to the target, often attaching personal details to their communications. The challenge for authorities, therefore, is identifying which abusive communications are most likely to develop into credible threats to an individual’s personal security, and directing resources towards the most dangerous perpetrators.

Research shows a very high prevalence of mental disorder within the population of fixated individuals who pursue public figures. A systematic 2009 study of 275 police-recorded cases of inappropriate communications or approaches to members of the British Royal Family found that 230 (83.6%) individuals in the sample were suffering from serious mental illness, typically of a psychotic nature. Of the sample, 175 (63.6%) displayed delusional beliefs, with 149 (54.2%) individuals demonstrating ‘grandiose ideas’.[11]

Similarly, a 2007 study examining all non-terrorist attacks on elected politicians in Western Europe between 1990 and 2004 found that ten of the total 24 attackers (41.7%) were psychotic, and that those with a mental disorder were responsible for most of the fatal and seriously injurious attacks.[12] These findings have significant implications for prevention, and in particular the role of psychiatric intervention in preventing mentally ill individuals from progressing to constitute a serious risk. This is discussed in more detail in Chapter II.

Beyond the threats posed by fixated individuals, coordinated campaigns involving a number of actors are rarer, but there is considerable evidence to show that new forms of coordinated threat have emerged in the past decade. These actions include coordinated trolling, through which politicians and public figures receive an overwhelming storm of hostile, abusive or

[10] See, for example, J Reid Meloy et al., ‘A Research Review of Public Figure Threats, Approaches, Attacks, and Assassinations in the United States’, *Journal of Forensic Sciences* (Vol. 49, No. 5, October 2004); James et al., ‘The Role of Mental Disorder in Attacks on European Politicians 1990–2004’; David V James et al., ‘The Fixated Threat Assessment Centre: Preventing Harm and Facilitating Care’, *Journal of Forensic Psychiatry and Psychology* (Vol. 21, No. 4, 2010).

[11] David V James et al., ‘Stalkers and Harassers of Royalty: The Role of Mental Illness and Motivation’, *Psychological Medicine* (Vol. 39, No. 9, September 2009).

[12] James et al., ‘The Role of Mental Disorder in Attacks on European Politicians 1990–2004’.

threatening messages sent by groups coordinating online.[13] While the active terrorist groups currently operating in Britain have shown little sign of intending to carry out systematic attacks on named public figures, this situation could change suddenly, adding a terrorist component to the existing array of threats. There is also increasing evidence of state-level coordination of threatening activity, with certain foreign governments organising and encouraging actors to sow disinformation and stir up anger. Andrew Parker, Director-General of the British Security Service (MI5), recently described the Russian state's 'well-practised doctrine of blending media manipulation, social media disinformation and distortion with new and old forms of espionage, high levels of cyber attacks, military force and criminal thuggery' as one of the primary hostile threats facing the UK in 2018.[14]

Victims

While energetic and challenging debate has always been an indispensable facet of the UK's parliamentary process, research shows that MPs, candidates, their support staff, volunteers, and families are frequently targeted by persistent abuse, especially directed towards women and those from ethnic and religious minorities. A 2016 survey-based study conducted by David James and colleagues found that of the 239 MPs who responded to the questionnaire, 192 (80.8%) had experienced at least one form of intrusive and aggressive behaviour, 101 (42.3%) reported that they had experienced threats to harm them or those close to them, while 90 (37.7%) reported being stalked. Of those who had experienced some form of intrusive or aggressive behaviour, 132 (72.9%) reported that they had been made fearful by their experience.[15]

In addition, a recent review conducted by the Committee on Standards in Public Life found that every female MP active on Twitter reported experience of online intimidation,[16] with several candidates reporting that they would not have stood for election if they had known the level of intimidation they would receive.[17] The report found that a new form of intimidation had emerged during the period of the 2017 general election, driven primarily by the use of abusive social media campaigns directed towards MPs and parliamentary candidates, concluding that 'social media is changing the way in which election campaigns are conducted and has led to a marked shift in how the public engages with Parliamentary candidates'.[18]

[13] Alex Krasodomski-Jones, 'Signal and Noise'; Committee on Standards in Public Life, *Intimidation in Public Life,* pp. 13–16; Susanna Every-Palmer, Justin Barry-Walsh and Michele Pathé, 'Harassment, Stalking, Threats and Attacks Targeting New Zealand Politicians: A Mental Health Issue', *Australian and New Zealand Journal of Psychiatry* (Vol. 49, No. 7, 2015).

[14] Andrew Parker, speech given to BfV Symposium, Berlin, 14 May 2018, <https://www.mi5.gov.uk/news/director-general-andrew-parker-speech-to-bfv-symposium>, accessed 16 May 2018.

[15] James et al., 'Aggressive/Intrusive Behaviours, Harassment and Stalking of the United Kingdom Parliament'.

[16] Committee on Standards in Public Life, *Intimidation in Public Life*, p. 27.

[17] *Ibid*., p. 29.

[18] *Ibid*., p. 27.

While on the one hand the internet has succeeded in politically engaging individuals who may not have previously participated in the democratic process, it has also emboldened those seeking to use these platforms for malicious purposes. The true extent of the problem is often underestimated by the public, and this has led to a widespread expectation that parliamentarians should simply 'shrug it off'. However, it is clear that a new trend of abuse, harassment and intimidation has emerged in recent years, and individuals in public life now face a more diverse range of threats, originating from a wider variety of sources.

However, systematic evidence on this phenomenon has not been collected until very recently, and these observations are somewhat anecdotal in nature. Further quantitative research is needed to assert with greater clarity the true scale of online intimidation towards public figures and its broader impact on the democratic process. Another limitation lies in the familiar issue of under-reporting: the prevalence of threats to different groups is likely to be conflated with differences in reporting thresholds. For example, newer MPs may be more likely to report abuse, giving the impression that they are more likely to be targeted.

Furthermore, while discussions have focused on the personal security of MPs, local councillors and local government employees are also vulnerable to a range of threats from members of the public, and in some respects are at greater risk. Unlike MPs, local councillors and council candidates are required to make their home addresses publicly available. In addition, local councillors are in many cases more closely engaged with the local community than MPs, and are subject to intense pressures in the form of physical intimidation, attempts to disrupt public meetings, and personalised attacks motivated by perceived local authority injustices. To date, these experiences have been poorly reported, and there is a lack of evidence on the true extent of this problem. Interviews with MPs who have experienced aggressive and unwanted behaviour suggest that they are 'sheltered from the experience' to a certain degree, with the most abusive correspondence not reaching them because it is intercepted by their staff.[19] The same is not true of local councillors and other government employees, who do not have the same support structure as MPs.

The Internet

The individuals and groups responsible for this activity have been quick to capitalise on the opportunities presented by the internet and social media, and as a result the threats have evolved significantly in scale and complexity. The anonymity offered by online platforms means that a larger number of individuals who would not otherwise consider engaging in abuse and intimidation offline are readily launching such attacks against public figures online, and with increasing coordination and sophistication.

[19] James et al., 'Aggressive/Intrusive Behaviours, Harassment and Stalking of the United Kingdom Parliament'.

Online abuse and intimidation may be perceived by perpetrators to be a consequence-free activity, due to the 'online disinhibition effect' and the perception of a low risk of consequences.[20] The impersonal nature of social media also means that casual trolls are unlikely to recognise the impact that their behaviour has on their victims. Research by Demos shows that throughout the EU referendum campaign period, around 1 in 20 of all messages sent to MPs were abusive.[21] As Labour MP and Shadow Home Secretary Diane Abbott described in February 2017, 'When I was a new MP if you want[ed] to send racist abuse you wrote a letter, in green ink usually, and you got maybe one or two of those letters a week. Now you can press a button and threaten to rape somebody'.[22]

The increase in the scale and volume of malicious communications has often overwhelmed the abilities of public sector stakeholders to respond. But technology can also be instrumental in enabling stakeholders to do more with the limited resources available to them, and the private sector has an important role to play in helping public sector agencies effectively respond to these new threats. Local police forces in particular are struggling to develop effective responses, due in part to a lack of training, as well as misunderstanding and disagreement over jurisdiction and responsibility, and limited awareness about the nature of the problem.[23] Shrinking police resources only compound the issue, with forces tending to prioritise their responses for cases where there is a potential threat to life.

Research for the Suzy Lamplugh Trust found that the internet has opened up a new range of opportunities for those intending to stalk.[24] The 2016 survey-based study of 4,054 British adults found that 18% of all women and 8% of all men reported being stalked, and that 36.8% of those who had been stalked reported that the stalker had used online methods. The research also found that, of those who had been stalked online, 43% had withdrawn from their online activity and/or social media usage. Where online stalking was the sole form of stalking behaviour reported, only 10% of people reported it to the police. These findings suggest that social media companies have an important responsibility to protect their users and secure their platforms from stalkers and those looking to harass and abuse.

Some have argued that further political pressure, or maybe even legislative change, may be required to address online threats to public figures. However, given the scale of the technology sector, a single legislative requirement may have unintended consequences elsewhere, or may punish cooperative technology companies as well as those more reluctant to act. Furthermore,

[20] For further discussion of the 'online disinhibition effect', see John Suler, 'The Online Disinhibition Effect', *CyberPsychology and Behavior* (Vol. 7, No. 3, July 2004).

[21] Krasodomski-Jones, 'Signal and Noise'.

[22] Francesca Gillett, 'Labour MP Diane Abbott: "Staff Try Not to Let me Out Alone in Hackney Because of Abuse Fears"', *Evening Standard*, 19 February 2017.

[23] Committee on Standards in Public Life, *Intimidation in Public Life*, pp. 65–69.

[24] Suzy Lamplugh Trust and Stalking Counts, 'Britain's First Nationwide Findings on Cyberstalking Released by Suzy Lamplugh Trust', media advisory, April 2016, <http://www.silverwoodbooks.co.uk/assets/docs/media kit - the stalker in your pocket.pdf>, accessed 16 May 2018.

achieving a strong negotiating position with the private sector will require first setting out a clear understanding of what constitutes acceptable use of an online platform, and the British government's expectations in this regard remain unclear.

It is also important not to overlook the progress that has been made in improving cooperation with the technology sector. Authorities responsible for protecting individuals in public life report that relationships with technology companies have improved in recent years, and that technology companies do assist with ongoing investigative work when they can. Data shows that between January and June 2017, Facebook provided data to authorities in more than 92% of cases when it was requested as part of legal process.[25]

However, there is mounting pressure from governments and law enforcement for social media companies to expand and enhance their automated takedown of abusive content. Assessing what constitutes abusive messaging inevitably involves a great deal of subjective judgement, and the experience that social media companies have of terrorist-related extremist content removal demonstrates the difficulties in developing automated systems that can accurately identify and remove abusive content.[26]

Moreover, while governments have argued that technology companies must take more responsibility for the safety and security of their users,[27] it is misguided to treat the internet and social media as the root cause of these problems. In the case of threats against parliamentarians, political parties must also work together to take greater responsibility for the behaviour of their members and supporters. The broadcast and print media also bear an important responsibility to ensure they do not incite intimidation through the use of threatening language and personalised attacks, inadvertently perpetuate online abuse campaigns by unnecessarily publicising them, or encourage others to obtain stories by way of harassment or intimidation.[28] In some cases the invasive nature of reporting on the private lives of individuals in public life could also result in information being released into the public domain that compromises their security.

Specialists in online radicalisation have pointed to the risks posed by newspapers and academics re-publishing terrorist propaganda under the guise of academia or news reporting with insufficient care paid to the potential risks.[29] Recent cases have shown the impact mainstream media can have on fixated individuals: Darren Osborne, the Finsbury Park terrorist who was found guilty of murder and attempted murder after driving a rental van into a crowd of Muslim worshippers in June 2017, is reported to have been radicalised in a matter of weeks by watching a BBC drama

[25] Facebook, 'Requests for Data: United Kingdom', <https://transparency.facebook.com/government-data-requests/country/GB>, accessed 8 May 2018.

[26] Alexander Babuta, 'Online Radicalisation: The Need for an Offline Response', RUSI Commentary, 25 September 2017.

[27] Committee on Standards in Public Life, *Intimidation in Public Life*, p. 14.

[28] *Ibid*., p. 19.

[29] Martyn Frampton with Ali Fisher and Nico Prucha, *The New Netwar: Countering Extremism Online* (London: Policy Exchange, 2017), p. 65.

on the subject of the Rochdale abuse scandal. The judge in the case is quoted as saying to Osborne, ‘your research and joining Twitter early in June 2017 exposed you to a great deal of extreme racist and anti-Islamic ideology’.[30] Osborne had previously intended to target Labour politicians Sadiq Khan and Jeremy Corbyn, whom he had described as terrorist sympathisers, echoing a number of digital and mainstream media headlines. This case exemplifies the role that traditional media can play in incidentally increasing the risk to public individuals, and underlines the difficulties facing editors in overseeing the content for which they are responsible.

[30] Kevin Rawlinson, ‘Darren Osborne Jailed for Life for Finsbury Park Terrorist Attack’, *The Guardian,* 2 February 2018.

II. Tackling the Threat and Protecting the Victims

Accessibility and Security

IN ANY ORGANISATION, it is impossible for most people to completely protect themselves from abuse or harassment, and in many professions, individuals are expected to remain readily accessible to the public. The growth of social media has only reinforced this expectation. Individuals in public life should therefore be made aware of the support they should expect to receive should they be targeted, and there should be more consistency across organisations and jurisdictions in the support available to victims.

Close protection delivered by police and security agencies is an extremely expensive endeavour, and it is necessary to carefully consider and prioritise which individuals should receive such services. Decisions on who to protect and how are obviously sensitive and therefore confidential. Some individuals receive protection by virtue of the assessed threat to their safety and security, while others are protected because of their job, role or position. However, while focusing efforts to protect these individuals from threats to their security, it is equally important not to overlook the safety of those around them, such as their close family and staff. While a very small number of national figures may have a structure of close protection around them, there is a large 'middle ground' of individuals in public life who do not have the same, or indeed any, support. Although research examining the safety of office holders' staff is limited, a survey-based study conducted by Timothy Lowry and colleagues in Queensland, Australia found that 67% of parliamentarians' staff reported experiencing at least one form of harassment.[31] The authors of the study stress the importance of formal training and security procedures for MPs' staff, a finding that is equally relevant to the UK.

Parliamentarians, ministers and members of the royal household face a dilemma in balancing accessibility and security: they are required to engage with the public and have outward-facing public profiles, which inevitably makes them vulnerable to members of the public who may wish to do them harm. In the case of politicians, they are also required to express opinions on current affairs and world events and voice these opinions as openly as possible. This invariably attracts those who hold contrary opinions, some of whom may be sufficiently motivated to resort to abuse or violence, or those who may have a mental health issue which leads them to wish harm on others.

[31] Timothy Lowry et al., 'Harassment and Other Problematic Behaviors Experienced by the Staff of Public Office Holders', *Journal of Threat Assessment and Management* (Vol. 2, No. 1, March 2015).

While Article 10 of the Human Rights Act 1998 states that every individual has the right to freedom of expression, including ‘freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers’, the exercise of these freedoms is nevertheless subject to ‘formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety’, or ‘for the protection of the reputation or rights of others’.[32] A careful balance must therefore be struck between preserving freedom of expression and protecting individuals in public life, and there will inevitably be situations where it is necessary to curtail individuals’ freedom of speech in order to protect the security and reputation of public figures.

Protecting individuals in public life from harm has also become significantly more difficult in recent years, as before the advent of the internet it was easier to maintain a veil of secrecy around public figures’ private lives. With the growth of the internet, members of the public are now able to collect a great deal of information about the private lives of public figures, and then share this information with a large number of potential perpetrators. In the past, collecting such information required perpetrators to engage in hostile reconnaissance activity, which put them at greater risk of detection by authorities, but many of these opportunities to detect such activity no longer exist. Today, technology companies potentially play an important role here, as they may be better placed than law enforcement to detect online activity related to stalking and attack planning, although questions remain as to the responsibilities and jurisdictions of large technology companies in fighting crime.

The Law

Legislation is an important measure to consider when protecting individuals in public life, and authorities require a comprehensive legislative framework that allows for effective enforcement against perpetrators. Some have suggested that existing legislation may need to be reviewed given the changing nature of the threat landscape. For instance, the review conducted by the Committee on Standards in Public Life suggested the introduction of a new electoral law prohibiting the intimidation of parliamentary candidates and party campaigners,[33] with Prime Minister Theresa May announcing in February 2018 that the government would consult on the introduction of such a law. However, the review also contradictorily found ‘no evidence to suggest that the current criminal law is insufficient in covering the full range of cases that we have defined as intimidation for the purpose of this report’, concluding that ‘the current criminal law should remain as it is’.[34]

There have also been suggestions that existing legislation should be updated to include criminal offences specific to social media. However, police officers consulted for the purposes of the

[32] ‘Human Rights Act 1998 (UK)’.

[33] Committee on Standards in Public Life, *Intimidation in Public Life*, p. 22.

[34] *Ibid*., p. 60.

aforementioned review claim that existing legislation is sufficient to prosecute for all relevant offences committed using social media, with Chief Constable Mike Barton reporting that:

> There is a view that, with the advent of the internet, some of our more ancient laws are probably not applicable, but we do not find that. For example, threats to kill comes from the Offences Against the Person Act 1861 and is perfectly serviceable. The Public Order Act 1986 is perfectly serviceable. The Malicious Communications Act 1988 was designed around telephones and letters and is perfectly serviceable. Broadly, we are content with that.[35]

In addition to the Malicious Communications Act 1988, the Protection from Harassment Act 1997 can also be used to prosecute individuals for repeated unwanted or intrusive communications.

Treating major technology companies as publishers (rather than platform hosts) has frequently been proposed by politicians and policymakers as an option in curbing digital threats. This would entail a fundamental redefinition of the way the web is used, and would likely be resisted by companies whose entire revenue model would be threatened. The technological, political and ethical challenges of demanding that digital public spaces are algorithmically and automatically censored by private corporations based abroad are manifold, particularly when a political motivation to be seen to be tough on the technology firms comes at the cost of workable policy. Such a move also appears unnecessary, with the report from the Committee on Standards in Public Life concluding that '[w]e have seen no evidence that the current criminal law is insufficient. New offences specific to social media are unnecessary and could be rendered outdated quickly'.[36]

It seems, then, that existing legislation is sufficient to prosecute for criminal offences committed against individuals in public life, whether online or offline. However, in order for legislation to be effective it relies upon consistent reporting by victims, as well as a willingness among law enforcement to prioritise investigating and pursuing offenders. Under-reporting and a lack of understanding about stalking and abuse among victims and throughout the criminal justice system both remain significant barriers to progress.

Understanding and Under-Reporting

As for many other forms of crime, research suggests that the vast majority of abuse and stalking goes unreported. A survey-based study of 4,054 British adults found that only 26.6% of all stalking cases had been reported to the police.[37] Research also indicates a lack of understanding among victims about what constitutes stalking and what support is available for victims. While a survey-based study conducted by David James and colleagues found that of the 239 MPs who responded to the questionnaire, 192 (80.8%) had experienced at least one form of intrusive

[35] *Ibid*., p. 59.

[36] *Ibid*., p. 16.

[37] Suzy Lamplugh Trust and Stalking Counts, 'Britain's First Nationwide Findings on Cyberstalking Released by Suzy Lamplugh Trust'.

and aggressive behaviour,[38] the Committee on Standards in Public Life found that Parliamentary candidates 'were not confident in recognising when intimidatory behaviour was likely to constitute a criminal offence', suggesting that guidance booklets distributed to candidates at the beginning of an election period should offer clearer guidance on this issue.[39]

It is important to develop processes for training new MPs and their staff on how to respond to potential threats, and ensure that those in the public eye recognise when they are being targeted by stalkers. MPs must have trust in the advice they are being given, and feel they are supported by a network of capable individuals and agencies who are on hand to provide support to them and their staff when needed. After all, MPs are there to serve the public, and the threat of abuse hinders their ability to effectively do so.

Research has also highlighted serious concerns regarding the police response to stalking. Of all British adults who reported some form of stalking to the police, 43.4% found the response to be not very helpful or not helpful at all.[40] The Committee on Standards in Public Life also found that 'there is currently inconsistency in the approach taken locally by police forces in policing intimidatory behaviour towards Parliamentary candidates', highlighting poor training and a lack of policing guidance as main barriers to progress in this regard.[41] Better education is needed throughout the criminal justice system to improve understanding about stalking and abuse, the risks posed to victims, and the importance of prioritising and investigating offenders. A single point of contact (SPOC) within each force that would take responsibility for stalking allegations could be an important practical step towards achieving greater consistency in the police response to stalking.

Multi-Agency Intervention Models

Given the multi-dimensional nature of the problem outlined above, addressing the many security threats faced by individuals in public life is not the responsibility of any single department, organisation or agency. Rather, a multi-agency approach is needed, that engages a range of stakeholders, facilitates collaborative working and streamlines data-sharing. Given the high prevalence of mental illness among those who pose a threat to public figures, the role of health trusts and psychiatric services is particularly important.

The Fixated Threat Assessment Centre (FTAC), established in 2006 by the Office for Security and Counter-Terrorism at the Home Office, Metropolitan Police Service and Department of Health, is the first joint police/National Health Service (NHS) unit in the UK, and operates as a police unit with full-time psychiatric NHS staff permanently embedded and working alongside police

[38] James et al., 'Aggressive/Intrusive Behaviours, Harassment and Stalking of the United Kingdom Parliament'.

[39] Committee on Standards in Public Life, *Intimidation in Public Life*, pp. 68–69.

[40] Suzy Lamplugh Trust and Stalking Counts, 'Britain's First Nationwide Findings on Cyberstalking Released by Suzy Lamplugh Trust'.

[41] Committee on Standards in Public Life, *Intimidation in Public Life*, p. 17.

officers. Studies of FTAC interventions and their outcomes show that this approach has been highly effective: David James and colleagues found that, of 100 FTAC cases that were assessed as moderate or high concern, 86% of individuals were found to be suffering from psychotic illness, and 57% were admitted to hospital as a result of FTAC intervention, with a further 26% receiving care from community mental health services.[42] A follow-up study by David James and Frank Farnham found that, following FTAC intervention, the proportion of individuals engaged in concerning behaviours decreased by around half, while the numbers of incidents of concerning behaviours decreased by around 65%.[43]

The FTAC model has since been adopted by agencies in Sweden, the Netherlands and Australia, a testament to its effectiveness and replicability.[44] Examples include the Queensland Fixated Threat Assessment Centre established in 2014,[45] the New South Wales Police Fixated Persons Investigations Unit set up in 2017,[46] and most recently the Victoria Police FTAC, established in February 2018 with an AUS$31.6 million government investment.[47] As well as delivering preventive interventions that seek to reduce risk in the overall population while also identifying the small number of individuals who pose the greatest threat, one of the model's core strengths is in facilitating data-sharing between police and partner agencies.[48] This is of particular importance in Britain, where data-sharing deficiencies between the police and partner agencies mean that the police's understanding of risk is currently somewhat one-dimensional.[49]

Thus far, support provided to victims of abuse and stalking has been inconsistent and uncoordinated, due to disagreements and misunderstanding over governance arrangements, ownership of responsibilities, duties of care, and accountability. The Multi-Agency Stalking Intervention Project (MASIP), delivered by the Suzy Lamplugh Trust and funded by the Police Transformation Fund via the Mayor's Office for Policing and Crime (MOPAC), is a promising step

[42] James et al., 'The Fixated Threat Assessment Centre'.

[43] David V James and Frank R Farnham, 'Outcome and Efficacy of Interventions by a Public Figure Threat Assessment and Management Unit: A Mirrored Study of Concerning Behaviors and Police Contacts Before and After Intervention', *Behavioral Sciences and the Law* (Vol. 34, No. 5, September/October 2016).

[44] Niall Boyce, 'The UK's Fix for Fixated Threats', World Report, *The Lancet* (Vol. 377, No. 9763, January 2011).

[45] Queensland Fixated Threat Assessment Centre (QFTAC), 'What is QFTAC?', <https://www.mhrt.qld.gov.au/wp-content/uploads/2014/02/QFTAC-brochure-original.pdf>, accessed 4 May 2018.

[46] Jessica Kidd, 'New NSW Police Specialist Unit Hopes to Intervene Before Lone-Wolf-Style Attacks', *ABC News*, 26 April 2017.

[47] Lisa Neville, 'New Centre to Prevent Lone Actor Attacks Unveiled', media release, 28 February 2018, <https://www.premier.vic.gov.au/wp-content/uploads/2018/02/180228-New-Centre-To-Prevent-Lone-Actor-Attacks-Unveiled.pdf>, accessed 8 May 2018.

[48] James et al., 'The Fixated Threat Assessment Centre'.

[49] Alexander Babuta, 'Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities', *RUSI Occasional Papers* (September 2017), p. 24.

towards achieving a truly multi-agency approach to victim support services.[50] The pilot project seeks to develop a multi-disciplinary partnership between police forces, health trusts, mental healthcare services, and victims' services to link up advocacy, casework and support to deliver a holistic package of support to victims of stalking in public life.

It is clear that the responsibility for policing the online space cannot lie purely with technology companies. One example of a successful multi-agency initiative is the Mayor of London's Online Hate Crime Hub,[51] which brings together law enforcement, government representatives, academics, victims, and the private sector to work together to address these online threats. Multi-agency efforts such as these are likely to be the most effective way of addressing online threats to public figures.

It is also important not to overlook the role of individual user behaviour on social media. There are certain measures and precautions social media users can take to preserve their security, such as disabling functionality that publishes their precise geolocation data in real-time alongside posts. Citizens therefore have a responsibility to ensure they use social media safely and responsibly, while social media companies themselves have an important role to play in providing education on the safe use of social media. Guidelines on safe use of social media could also be included in the basic protective security package provided to MPs.

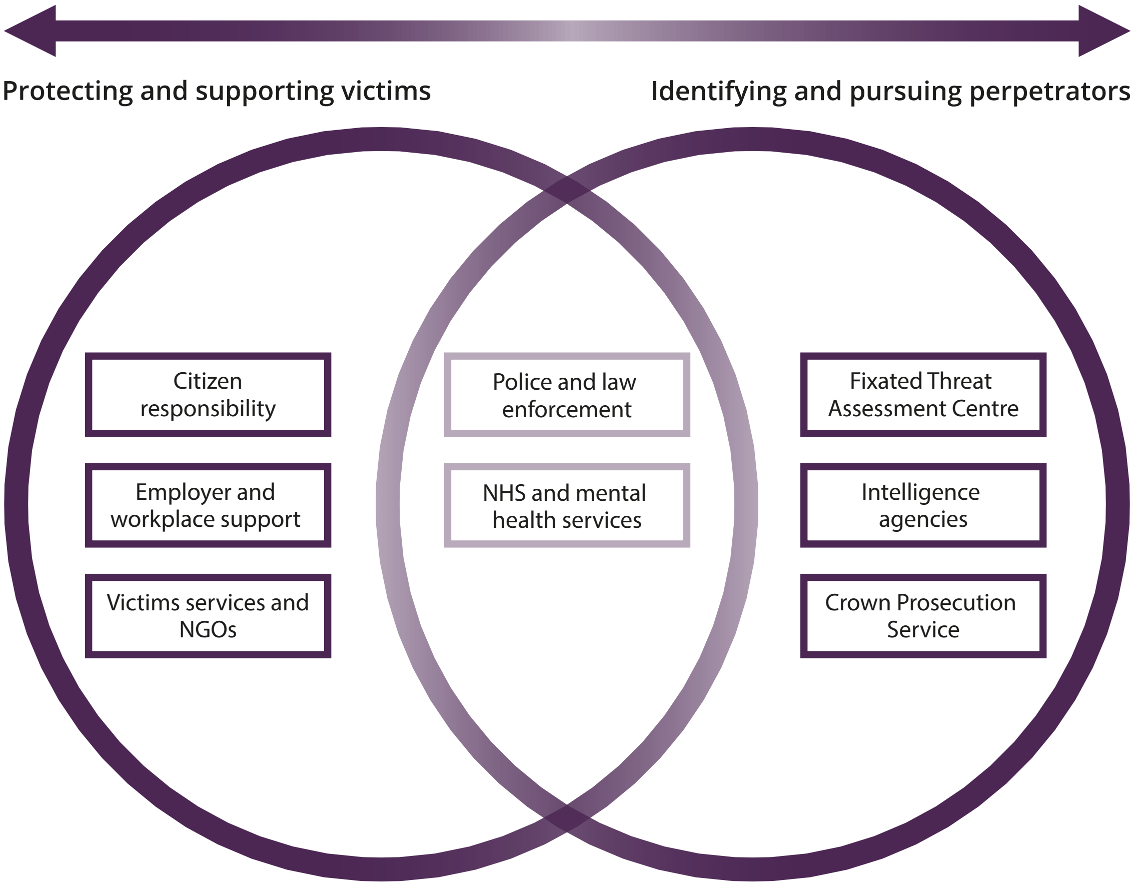
While a number of promising new multi-agency approaches have been developed in recent years, these initiatives require significant, sustained resources from central government, and given the current economic and security climate both nationally and internationally, there is a risk that initiatives may not receive the ongoing support they require. Furthermore, local and regional initiatives may not be rolled out nationwide, and there remains inconsistency across the country in the level of support available to victims.

Based on the issues discussed above, the division of responsibilities for those tasked with protecting individuals in public life and identifying and pursuing perpetrators can be broadly understood from the following chart (Figure 2).

[50] See Suzy Lamplugh Trust, 'Multi-Agency Stalking Intervention Programme', <https://www.suzylamplugh.org/multi-agency-stalking-intervention-programme-masip>, accessed 16 May 2018.

[51] Mayor of London and London Assembly, 'Mayor Launches New Unit to Tackle Online Hate Crime', press release, 24 April 2017, <https://www.london.gov.uk/press-releases/mayoral/mayor-launches-unit-to-tackle-online-hate-crime>, accessed 8 May 2018.

Figure 2: Division of Responsibilities


Protecting and supporting victims
Identifying and pursuing perpetrators
Citizen responsibility
Employer and workplace support
Victims services and NGOs
Police and law enforcement
NHS and mental health services
Fixated Threat Assessment Centre
Intelligence agencies
Crown Prosecution Service

Source: The Authors.

The '4 Ps': Protect, Prepare, Prevent, Pursue

The '4 Ps' approach adopted by the UK's CONTEST Strategy for Countering Terrorism may provide a useful framework for developing responses to the threats facing individuals in public life, while recognising that the threats are very different in nature.[52]

The 'Protect' strand is perhaps of most relevance here,[53] as the primary aim is to protect individuals from coming to harm. For countering terrorism, 'protect' involves securing infrastructure and public spaces from potential attacks, and increasing the resilience of physical structures. Applying these principles to this context, 'protect' duties include: ensuring that

[52] HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (London: The Stationery Office, 2011).

[53] *Ibid*., pp. 78–91.

individuals' places of work are sufficiently secure to prevent potential attackers from gaining access; delivery of close protective security services in the case of high-profile public figures; and adopting cybersecurity protocols and privacy settings to increase resilience in the online space. Social media companies have a clear role to play here in improving the security of online platforms. New safety mechanisms could be introduced that detect hostile or offensive material and prevent it from being shared on certain pages, similar to the 'safesearch' feature used on most internet search engines. While automated content removal systems are likely to be impractical in this context, social media companies could nevertheless make more effective use of big data capabilities to identify online abuse and ban the accounts and IP addresses of persistent offenders, making social media platforms more hostile environments for would-be attackers.

Under 'Prepare',[54] clear processes and structures must be in place for individuals to report when they have been targeted by abuse, harassment or other forms of attack. Preparing for an attack requires that there are standardised mechanisms through which individuals can report offences, where those reports are then passed on to the relevant agency or department to investigate and escalate the matter if necessary. For most private citizens, the relevant agency will usually be their employer (or school, in the case of children). 'Prepare' in this context could also refer to training and awareness campaigns to inform individuals of how best to respond when they are targeted by abuse or harassment, how to de-escalate threatening situations, and how to identify the signs that they may be the target of stalking. While information and training provided to parliamentarians and their staff on how to identify and manage security threats has improved in recent years, uptake is reportedly inconsistent, with recommended security precautions often not being implemented in practice.

'Prevent' in the context of counterterrorism seeks to deliver early interventions to prevent individuals from developing extremist ideologies and radical beliefs.[55] In the context of threats to public figures, the role of psychiatric intervention is perhaps of greatest relevance. Research has demonstrated the high prevalence of mental illness among those who launch or attempt to launch attacks against public figures.[56] Based on these findings, James and colleagues suggest that rather than attempting to identify the very small proportion of individuals who may go on to commit acts of violence, a more appropriate approach may be to reduce the overall risk in the population.[57] This is achieved by ensuring the delivery of population-wide mental health interventions to prevent the high-risk cohort from progressing to acts of violence without them needing to be individually identified.[58] The 'public health approach' to violence prevention has already proved successful in a range of contexts,[59] and the guidelines produced by the Centers

[54] *Ibid*., pp. 92–103.

[55] *Ibid*., pp. 58–72.

[56] James et al., 'Stalkers and Harassers of Royalty'; James et al., 'The Role of Mental Disorder in Attacks on European Politicians 1990–2004'.

[57] James et al., 'Stalkers and Harassers of Royalty'.

[58] James et al., 'The Fixated Threat Assessment Centre'.

[59] See, for example, World Health Organization, *Violence Prevention: The Evidence* (Geneva: WHO Press, 2010); Linda Dahlberg and Etienne Krug, 'Violence: A Global Public Health Problem', in

for Disease Control and Prevention provide a useful framework for mental health practitioners seeking to prevent acts of violence and other criminality among those with poor mental health, which will in turn reduce the level of threat to public figures.[60]

In addition to the population-wide 'public health approach' to reducing the risk of violence committed by mentally ill individuals, the FTAC model also seeks to identify specific individuals who may be planning to engage in acts of violence and to deliver interventions to disrupt and deter them from doing so. As discussed previously, when individuals in public life have come to serious harm, the perpetrator has usually left a trail. Violent behaviour is typically preceded by abusive or intrusive communications and other forms of 'leakage', and fixated individuals often make themselves personally known to their victims. For this reason, there may be opportunities to detect behaviour related to attack planning, and to identify individuals who are mobilising towards acts of violence. This approach must be evidence-based and incorporate statistical methods in combination with structured professional judgement. The Communications Threat Assessment Protocol (CTAP-25) is one such statistical evaluation tool for practitioners to assess whether malicious communications are indicative of attack planning.[61]

For authorities to be able to identify those individuals who pose the greatest risk, individuals in public life have an important responsibility to report fixation-related behaviour that may be indicative of stalking. In the online space, social media companies may be better placed than state authorities to identify individuals who are demonstrating potentially concerning behaviour. The issue of this approach is the familiar problem of 'false positives' – many public figures are inundated daily with a constant stream of online abuse and bullying, and it may prove difficult to identify the small cohort of individuals who pose a credible threat to their safety.

'Pursue' in the context of counterterrorism refers to the ability of state authorities to investigate, apprehend and prosecute perpetrators.[62] In the context of threats to public figures, developing effective capabilities requires first that the division of responsibilities is clearly defined. In most cases, the responsibility will not rest solely with a single agency throughout the entire process, which is why effective collaboration and data-sharing mechanisms are essential. The FTAC

Etienne Krug et al. (eds), *World Report on Violence and Health* (Geneva: WHO Press, 2002), pp. 1–56; David Hemenway, 'The Public Health Approach to Violence Prevention', in Lydia Voigt, Dee Wood Harper and William Thornton (eds), *Preventing Lethal Violence in New Orleans, A Great American City* (Lafayette, LA: University of Louisiana Press, 2015); Dariush Mozaffarian, David Hemenway and David Ludwig, 'Curbing Gun Violence: Lessons from Public Health Successes', *JAMA* (Vol. 309, No. 6, 2013), pp. 551–52.

[60] Centers for Disease Control and Prevention, 'The Public Health Approach to Violence Prevention', <https://www.cdc.gov/violenceprevention/overview/publichealthapproach.html>, accessed 9 May 2018.

[61] David James, Rachel MacKenzie and Frank Farnham, *Communications Threat Assessment Protocol* (London: Theseus LLP, 2014).

[62] HM Government, *CONTEST*, pp. 44–56.

model provides an effective and useable framework to facilitate this and could potentially be expanded to include other organisations, such as the intelligence agencies and local authorities.

There are, however, limitations. In the case of ‘Pursue’, the clearest of these is the question of jurisdiction. Perpetrators of abuse and harassment may fall outside the legal jurisdiction of any responsible authority, particularly online. Technological problems are also present: data may be withheld when stored outside the UK’s legal jurisdiction. Although the major internet companies have shown a willingness to work with law enforcement, there are more exceptions than adherents to the rule. For instance, Telegram, a popular messaging app developed in Russia, has publicly stated it is not willing to work with law enforcement, and many similar apps are also available. In addition, the volumes of some threatening activities, such as cyberbullying and trolling, would require the commitment of resources that may be better allocated elsewhere.

Conclusion

THIS PAPER HAS examined the personal security of individuals in British public life, with specific focus on politicians and government employees. This is a complex and multi-faceted issue, and many research questions remain beyond the scope of this paper.

Threats to public figures range from casual 'trolling' and other unpleasant communications that are not necessarily illegal to serious offences such as physical assault and murder. In many cases the threats also include a dimension of discrimination, meaning they may fall within the scope of hate crime legislation. At the less severe end of the spectrum, the harm caused to victims amounts to psychological distress and personal offence, while more serious threats can cause individuals to withdraw from public life and may prevent them from effectively carrying out their public functions.

In recent years the threat to public figures has evolved significantly, driven primarily by the growth of the internet and social media. The anonymity offered by online platforms has reduced barriers to entry, meaning that more individuals are engaging in abusive behaviour than ever before. In response, many policymakers have called for stricter regulation on social media companies, for instance by treating them as publishers rather than platform hosts. However, these suggestions would be problematic to implement in practice, and the evidence suggests that existing legislation is sufficient to prosecute individuals when an offence has been committed. A greater challenge is in ensuring consistent reporting by victims, and willingness among law enforcement to prioritise and investigate potential threats. Improving education and awareness among public figures and throughout the policing and criminal justice system is therefore likely to be a more effective approach than attempting to introduce new legislation, which does not appear necessary.

While social media trolls and disaffected members of the public are perhaps the most voluminous category of perpetrator, research shows that the most serious threat to the security of individuals in public life comes from 'fixated loners'. A striking finding in this line of research is the very high prevalence of mental illness among fixated individuals who commit or attempt to commit attacks on public figures. This observation suggests that psychiatric services have an important role to play in prevention, by combining two complementary approaches. The first is the 'public health' model of population-wide risk reduction: by delivering psychiatric intervention measures to those who display symptoms of psychotic behaviour and other characteristics of fixation, the overall risk to public figures can be reduced without having to individually identify those who may be planning to engage in acts of violence. The second approach involves using intelligence assessment methods and other forms of data analysis to identify those individuals who pose the greatest potential security threat, and delivering targeted interventions to prevent and disrupt their planned activity. The FTAC model is a successful example of one such multi-agency initiative that has since been replicated overseas.

Given the broad range of threats, which vary in their prevalence and severity, together with the multitude of potential perpetrators, multi-agency initiatives are crucial to ensure victims receive the support they need. There is potential to build on the successes of a number of existing initiatives to engage more closely with other agencies, such as local authorities, and work with technology companies to facilitate regular dialogue and information sharing regarding potential security threats.

About the Authors

Alexander Babuta is a Research Fellow in the National Security and Resilience studies group at RUSI. His research focuses on policing and security in the digital age, transnational organised crime and counterterrorism.

Alex Krasodomski-Jones is a researcher at CASM (Centre for the Analysis of Social Media) at Demos. He has led research efforts into digital politics, disinformation, conspiracy theories, and the attention economy.