Welcome to this week's edition of Defuse News

A weekly briefing for people whose profile attracts attention.

Random or Targeted:
The Distinction That Shapes Everything

Ann Widdecombe was attacked in her own home, in a quiet Devon village, in the middle of the day. She was found the following day, having failed to appear for a television interview. Counter terrorism police have confirmed it was a targeted attack, and searches of the suspect's home found evidence of planning. The investigation continues, and I will not speculate on motive. But one word in the police statement should shape every conversation that follows: targeted.

The single most important distinction in protective work, the one that determines whether any measure you take will work, is the difference between random violence and targeted violence. Most of the security industry blurs it. Having founded The Parliamentary Liaison and Investigation Team (PLaIT) after Jo Cox was murdered, I can tell you this distinction is where prevention lives or dies.

Two different problems

Random violence is the drunk outside the venue, the opportunist who sees a chance and takes it. Against this, visible close protection works. A capable presence raises the cost of acting on impulse, and the opportunist moves on. Close protection deserves full credit for this.

Targeted violence is a different problem. The targeted attacker has chosen you. They have researched where you live, when you are alone, what your routines are. They pick the time and the place precisely to avoid whatever protection you have. In case after case, the attacker closes the distance before any protector can react. The engagement is over in seconds, and the planning that made it possible happened weeks earlier, unseen. Very few targeted attacks anywhere have been stopped by a protector drawing a weapon.

And here is the most uncomfortable truth of all. Through that research, the attacker often knows more about your security than you do. They have studied your cameras, your gates, your gaps and your habits with a focus you have never applied to them yourself, because for you it is background and for them it is the whole project.

The attack itself is only the final act of a long process. If your entire defence stands at the final act, you have surrendered every earlier chance to intervene, and those earlier chances are where targeted attacks are prevented.

Prevention starts on the pathway

Police found evidence of planning in this case, which is consistent with everything we know about targeted violence. Some attackers snap. Targeted attackers do not.

They travel a recognised pathway: a grievance forms, ideation follows, then research and planning, then preparation, then the breach and the attack. Danger

peaks long after the warning signs first appear, and at almost every stage there is observable behaviour: leakage of intent, communications shifting from venting to planning, approaches and probing.

The pathway runs both ways. Skilled early intervention takes people off it. **Acting early is prevention; acting late is merely response.**

Adapted with kind permission from F.S. Calhoun and S.W. Weston

Hunters and howlers

A word on who to worry about. Threat assessors distinguish between hunters and howlers. Howlers make noise: they threaten, abuse and alarm, yet very rarely attack. Hunters rarely howl: they research, plan and prepare in silence. US Secret Service research found that most attackers never communicated a direct threat to their target. A threat alone is a poor indicator of an impending attack, yet so often the professionals follow the noise and miss the hunter.

A warning here. Organisations often tell me they hold intelligence on the people fixated on their principal. When I ask what it tells them, the answer is a count of online threats and fixated individuals.

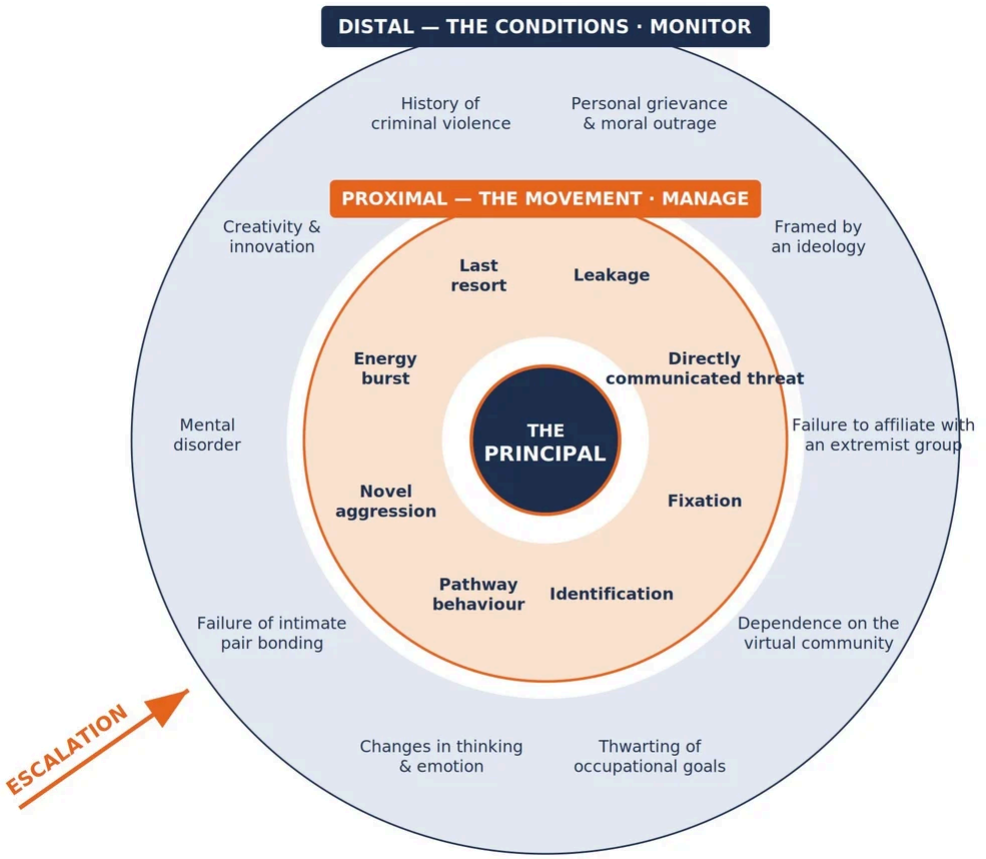
That is data. **Intelligence answers the question: so what?** Who is moving from thinking to doing? Whose behaviour is escalating? Without assessment, flagged accounts are noise that makes people feel monitored without making them safer.

From conditions to intent

So how do professionals tell the difference? By separating the conditions from the behaviours.

The conditions, what assessors call distal characteristics, are the background: a grievance, an ideology that frames it, personal failures and losses, a history of violence. They describe a person of concern rather than an imminent threat, though they are often what triggers the movement.

The behaviours, the proximal warning signs, are the movement itself: fixation on the target, research and probing, leaking intent, a direct threat. Conditions are monitored. Behaviours are managed. When a person moves from the conditions to the behaviours, they are escalating, and that is the moment to act.



Indicators from the TRAP-18 — Dr J. Reid Meloy (Meloy & Gill, 2016). **www.defuseglobal.com**

Be hard to find

The attack happened at home, the one place we all assume is ours, and for most prominent people the softest point in their entire security picture. A public figure's address, routines and family details are usually discoverable in an afternoon. What once took weeks of physical surveillance can now be assembled from open sources and data brokers in minutes. **Every targeted attack begins with research**, so every piece of information you remove from circulation is a genuine protective

measure. You can be a public figure without everyone knowing everything about you, but only if you deliberately audit and reduce what is out there.

Even harder to target

Then the physical layer, which costs little and is almost always missing. Ask yourself: if someone came through the door, how long until police arrive? In a rural village, considerably longer than you think. What is the plan for those minutes?

- A room you can retreat to, with a solid door
- A means of communication that does not depend on the phone in your hand
- A written note of the numbers that matter
- Detection that warns you, rather than merely recording the aftermath

Unglamorous measures, and the ones that decide outcomes.

Feeling safer is the actual job

In the UK, a physical attack remains a low probability, even for public figures. The corrosive effect of threat itself is not: the abuse, the fixated correspondence, the slow narrowing of a life lived on guard. The harm arrives long before any attacker does, and usually instead of one.

And whether a person feels safer is a huge factor in whether any security programme succeeds at all. Security only works if the person lives with it, and people abandon measures that make them feel watched or imprisoned.

The protocol gets skipped, the officer stood down for the school run, until the programme exists on paper only. Fear damages from the other direction too: a person who still feels unsafe stops reporting the odd letter or the strange car, and prevention starves without that information. A programme that protects the body while ignoring the mind fails twice.

Our mission

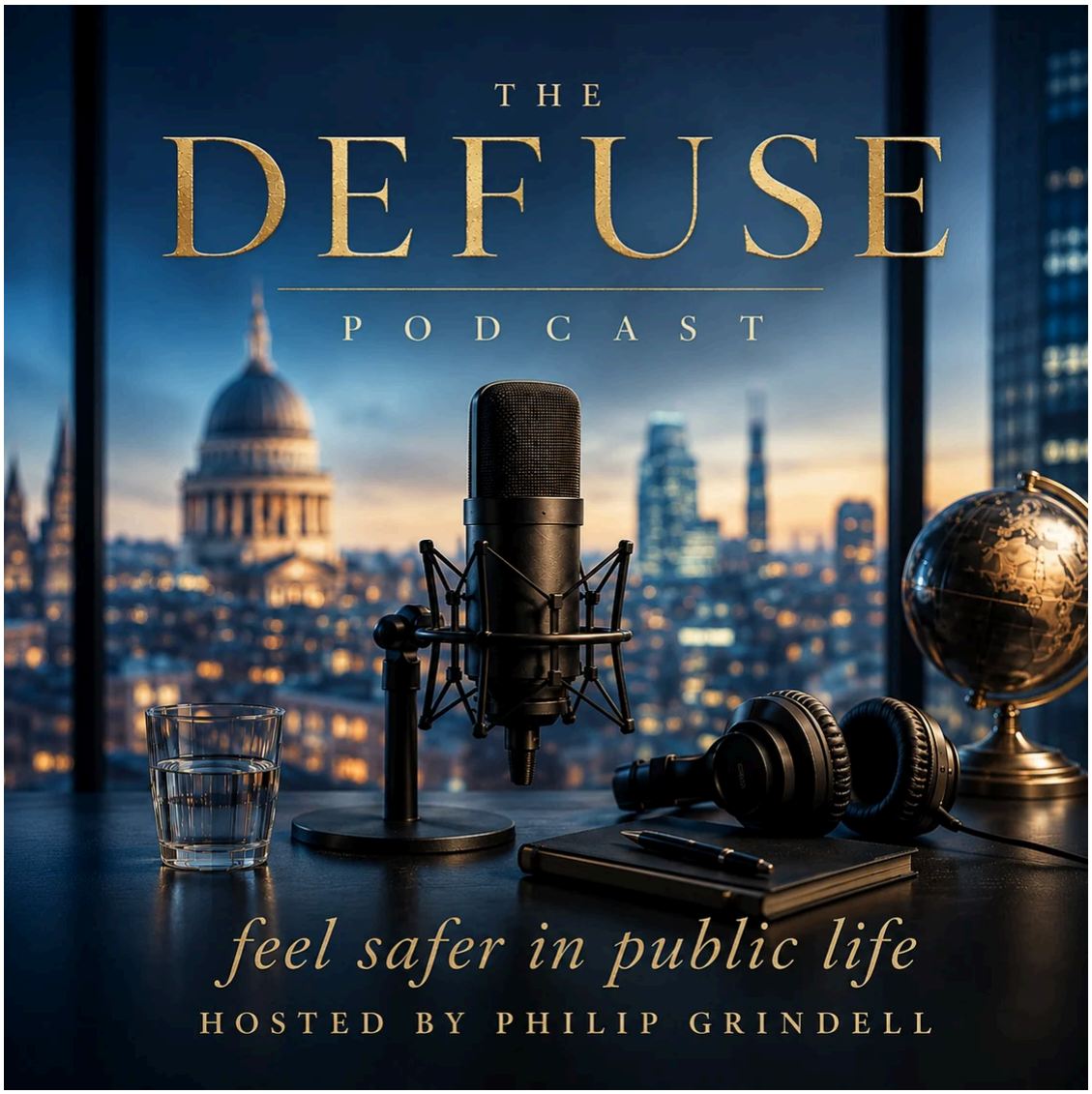
That is why "feel safer in public life" has always been Defuse Global's strapline. Keeping a public figure safe is relatively easy, provided they are willing to live inside a claustrophobic security programme that shrinks their world to what it can control. Helping them flourish, living fully and feeling safe while doing it, is a far harder job, and it is the one that actually matters.

The protective lesson from this tragedy is older than the case itself. Targeted attacks are preceded by observable behaviour and enabled by available information. Prevention means acting on the first and reducing the second

If this case has prompted you to wonder about your own exposure, that instinct is the right one. Every targeted attack begins with research. If someone became fixated on you or your family, how much could they already find?

Our Digital Exposure Assessment shows you exactly what is publicly available about you and your family, what someone with hostile intent could do with it, and a prioritised plan for reducing it.

Click here to find out what is already exposed.



Coming this August

Stop Waiting for the Threat, with Chuck Tobin

Philip is joined by a good friend. Chuck Tobin, President of AT-RISK International, is one of the most influential figures in protective security worldwide: a past President of the Association of Threat Assessment Professionals, current President of the International Protective Security Board, and the man who chaired the ASIS council that published the industry's first standard in executive protection. He is also someone Philip counts as a friend and a mentor, so what follows is two colleagues comparing notes, not an interview with a stranger, on a profession they both want to make better.

Together they take apart some of the industry's most persistent myths. Why 'threat assessment' is framed wrong from the start, teaching people to wait for a threat when the behavioural warning signs appear far earlier. Why the gun is not the answer: almost no attacks on principals have been stopped by a protector drawing a weapon, and with AI now compressing months of hostile surveillance into a targeting package built in minutes, surveillance detection has overtaken presence as the critical protective effort.

They also get practical, and uncomfortable. The executive with cameras and gates but no plan for the five minutes between calling the police and the police arriving.

The expensive safe room that fails in the first five minutes. The phone that holds your entire life, including the backup codes a thief now controls. And the question almost nobody asks: what harm are you actually exposed to, when reputational, psychological and financial damage are far more likely than physical attack?

A conversation about selling people what they need, rather than what the industry wants to sell them.

Chuck Tobin

Chuck Tobin has served as President of AT-RISK International since 2003, bringing over 35 years of experience protecting people, property and operations for clients worldwide. He leads complex threat investigations and executive protection risk assessments, and chaired Standards and Guidelines on the ASIS Executive Protection Council, publishing the industry's first standard in executive protection.

He is the current President of the International Protective Security Board, served as President of the Association of Threat Assessment Professionals from 2013 to 2017, and has been a volunteer leader for ATAP since 1999. He is a recipient of the

Florida Department of Law Enforcement Commissioner's Medal for his work advancing threat assessment.

📩 Know someone who would benefit from this newsletter?

Please send it to them.

Most people receive their first warning sign long before they receive any advice on what to do about it.

📫 Subscribe to Defuse News 🔗 defuseglobal.com/newsletter

- ✓ Free to subscribe
- ✓ Delivered every Monday morning
- ✓ Unsubscribe at any time

Philip Grindell MSc CSyP

Founder & CEO, Defuse Global

Author of **Personal Threat Management: The Practitioner's Guide to Keeping Clients Safer**

If anything in this newsletter has caused you to think, you may benefit from our help.

Contact us at info@defuseglobal.com