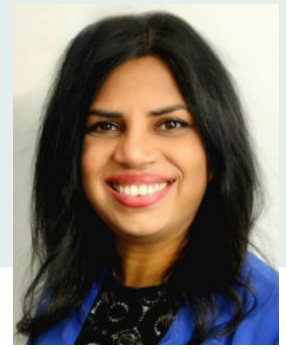


Cyber violence against women and girls must be treated as a national strategic priority



Dr Anitha Chinnaswamy

Director, GRIIT Network
Project Lead, CyVAWG and CyberDIVA
Aston University

Violence against women and girls is now firmly recognised as a national priority in the UK. Cyber violence must be treated with the same strategic seriousness. Evidence emerging from the CyVAWG and CyberDIVA projects shows how digital harms are reshaping abuse, outpacing institutional responses, and exposing the urgent need for stronger evidence, specialist capability, and cross-sector policy coordination.

VAWG is a matter of national strategic importance

Violence against women and girls is no longer being framed merely as a social harm at the margins of public policy. In 2024, police chiefs declared VAWG a national emergency, and the National Police Chiefs' Council now state that it accounts for just under 20% of all recorded crime in England and Wales. The government has also committed to halving VAWG within a decade, placing the issue firmly within national strategy rather than treating it as a discrete specialist concern. [1,2]

The issue is no longer simply whether institutions are aware of the problem, but whether the UK has built the systems, workforce and operational readiness required to respond effectively. This matters especially because the nature of violence itself is changing. Increasingly, abuse is mediated, amplified and prolonged through digital technologies. Digital abuse is not a secondary or less serious layer of harm. It is one of the principal environments through which coercion, humiliation, surveillance, intimidation, and sexual violence are enacted. The online and offline dimensions of abuse are now deeply entangled, and policy that treats digital harms as an adjunct to 'real-world' violence will continue to underperform.

Technology is reshaping the nature of harm

Technology-facilitated abuse spans online harassment, cyberstalking, image-based abuse, coercive monitoring, sextortion, doxxing, coordinated pile-ons, and AI-

generated sexual deepfakes. These harms differ from many conventional forms of abuse in three important respects: they travel faster, they persist longer, and they scale more easily. A single act can be replicated, archived, redistributed, algorithmically amplified, and made visible to multiple audiences at once. The resulting harm is often cumulative, reputational, and difficult to contain.

In February 2026, the Prime Minister recognised this reality, stating "the online world is the frontline of the 21st century battle against violence against women and girls," as new measures were announced requiring tech firms to remove flagged non-consensual intimate images within 48 hours. New measures on intimate image abuse, platform responsibility, and the protection of children from misogynistic online influences signal that the digital sphere is now central to the VAWG agenda. Yet recognition has run ahead of infrastructure needed to protect women and girls.[3,4]

Why CyVAWG and CyberDIVA matter in this policy landscape

CyVAWG, a multidisciplinary Innovate UK-funded project developed with support from the Department for Science, Innovation and Technology and West Midlands Police, was designed to strengthen understanding of cyber violence against women and girls and to improve prevention, reporting, awareness, and resilience. Its value lies not simply in the fact that it produced resources, but in the model it demonstrated: by bringing together insights from cybersecurity, law, policing,

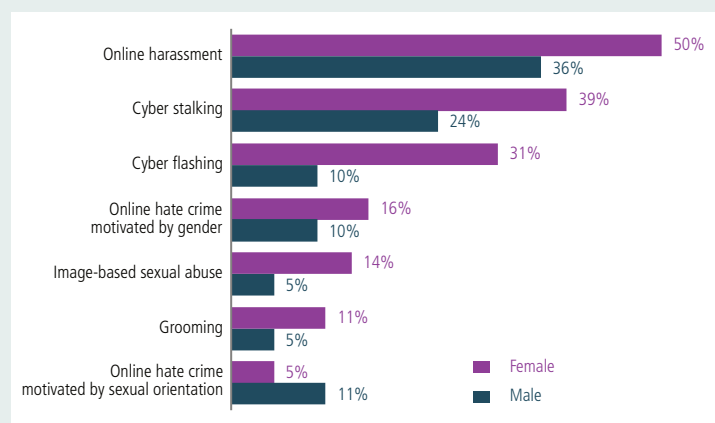
psychology, public policy and lived experience the developed resources were survivor-informed, interdisciplinary, policy-facing, and grounded in real operational need.[5] That combination is essential because cyber violence against women and girls cannot be adequately understood through any single disciplinary lens. It is simultaneously a justice issue, a safeguarding issue, a digital governance issue, a public health issue, and an education issue.

CyberDIVA is now advancing the field from awareness and response into forensic and evidence-led investigation. It examines cyber-enabled gender-based harm across both visible and hidden online environments, with a particular focus on the patterns, infrastructures, and tactics that enable abuse to proliferate. The project generates actionable evidence: forensic reporting, AI-enabled analytical tools, survivor-centred resources, a CyberDIVA toolkit (Figure 2), and practical guidance for law enforcement, regulators, and support organisations. It addresses a core problem that weakens national response – the gap between recognising the threat and being able to detect, analyse, and act on it consistently.[6]

The evidence gap is a strategic weakness

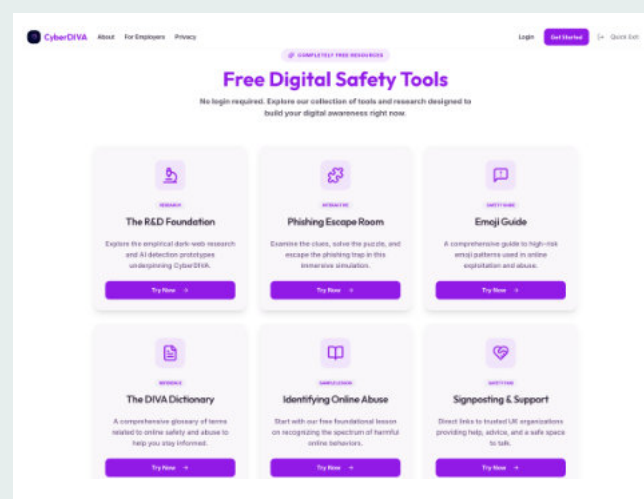
Across the UK, cyber violence against women and girls remains under-measured, inconsistently recorded, and unevenly interpreted. This is more than a technical limitation. Poor data architecture produces poor policy architecture. When incidents are categorised differently across

Figure 1. Type of abuse experienced among victims of online abuse, UK



Source/note: Victims' Commissioner (20 January to 27 February 2022), Statista, 2026. Respondents who were victims of online abuse, n=534

Figure 2. CyberDIVA toolkit



organisations and sectors, we lose the ability to compare cases, identify emerging patterns, evaluate interventions, and allocate resources intelligently.

In practice, women and girls encounter fragmented systems: different reporting routes, different thresholds for action, different understandings of digital evidence, and different levels of support. Research and stakeholder engagement repeatedly show that survivors often face an accumulation of barriers produced by institutional fragmentation. If VAWG is to be approached as a strategic national challenge, then cyber violence against women and girls must be supported by a common evidence framework robust enough for operational use and nuanced enough for survivor-centred practice.

Capability: the missing ingredient

The UK is not short of concern or actors. The deeper problem is capability. Many frontline systems still lack the specialist skills needed to recognise online abuse pathways, preserve digital evidence, understand platform logics, assess AI-enabled harms, and respond in ways that match the speed and complexity of contemporary abuse.

This points to the need for a capability agenda as well as a policy agenda. Addressing cyber violence against women and girls requires investment in specialist training, digital forensics capacity, interdisciplinary partnerships, and workforce development across sectors. No other fast-evolving national risk would be treated as manageable without building institutional competence around it. CyVAWG and CyberDIVA point to the

same lesson: durable progress depends on embedding expertise, not merely publishing statements of intent.

What parliament should prioritise now

1. **Supporting a common national data framework** for cyber violence against women and girls, with clearer definitions, stronger recording standards, and safer mechanisms for cross-sector insight sharing.
2. **Investing in specialist capability** across policing, education, local government, victim services, and the wider justice system.
3. **Backing sustained interdisciplinary infrastructure** that connects digital forensics, social science, policy, and survivor-centred practice, rather than relying on short-term and fragmented interventions.
4. **Pressing for stronger platform accountability**, including safety-by-design, faster redress mechanisms, and more transparent responses to harms that disproportionately affect women and girls.

The UK also needs to view this issue internationally. The technologies that facilitate abuse are transnational, platform-based, and rapidly evolving. The policy response must therefore be outward-looking and globally informed. The UK's wider commitment to putting women and girls at the centre of national and international policy should be matched by a clear ambition to lead on evidence-based, technology-aware responses to digital gender-based violence.[2,7]

Conclusion

Cyber violence against women and girls should not be treated as a niche sub-topic within the VAWG agenda. It is one of the defining policy and operational challenges now shaping that agenda. The significance of CyVAWG and CyberDIVA is that they show what a more serious response can look like: interdisciplinary, survivor-informed, technologically literate, and oriented towards real-world implementation.

Recognising VAWG as a national emergency was an important political step. The next step is to build the evidence systems, specialist capability, and institutional partnerships that allow the UK to respond effectively in both physical and digital space. If the UK is serious about prevention, protection, and justice, cyber violence against women and girls cannot remain peripheral. It must be central.

References

1. National Police Chiefs' Council. Violence Against Women and Girls. NPCC.
2. UK Government. Freedom from violence and abuse: a cross-government strategy. GOV.UK. Published 18 December 2025.
3. UK Government. VAWG strategy to better protect children from misogyny and abuse. GOV.UK. Published 19 December 2025.
4. UK Government. Tech companies must go "above and beyond" to protect women and girls from online abuse or face further action. GOV.UK. Published 10 March 2026.
5. GRIIT Network. CyVAWG (Cyber Violence Against Women and Girls). Project page.
6. GRIIT Network. CyberDIVA (Cyber Violence Investigation using Digital and Forensic Approaches). Project page.
7. UK Government. The UK is putting women and girls at the heart of everything that we do, from development to diplomacy: UK national statement at the UN Commission on the Status of Women. GOV.UK. Published 12 March 2025.