A TANGLED WEB: RETHINKING THE APPROACH TO ONLINE CSEA

A proposal to tackle the growing threat of online child sexual exploitation and abuse
## CONTENTS

**FOREWORD FROM NICK NEWMAN** 3

**INTRODUCTION** 5

We need to re-think the collective response to online CSEA 6

How to enhance the collective response to online CSEA 9

**SURVEY FINDINGS** 11

Coordination is a key challenge for all contributors 12

Government perspectives 14

Law enforcement and intelligence perspectives 16

Technology industry perspectives 18

Third sector perspectives 20

**RECOMMENDATIONS** 23

Tackling CSEA requires an orchestrated response 24

Adopt a tailored approach to the three tiers of threat 26

Disrupt the large-scale criminal orchestration of CSEA on the dark web 28

Direct proportionate and balanced regulation of the surface web 30

Educate children to enhance online CSEA prevention 32

**ABOUT THE SURVEY** 34

**AUTHORS** 35
Barely a week goes by without media coverage centring on online harms, from extremism and ‘hate speech’ to self-harm, cyberbullying and revenge pornography. After a decade-long debate between the proponents of security and privacy, the conversation has shifted to how we keep citizens safe online. We believe the highest priority should be tackling online child sexual exploitation and abuse (CSEA) given its scale, growth, rapidly evolving nature and devastating, life-long impact on the most vulnerable in our society.

As a founding industry member of the WePROTECT Global Alliance (see page 7), we have been working for five years with experienced practitioners in this field, from policy makers, law enforcement officers, industry partners and the third sector. We helped WePROTECT compile its first Global threat assessment to raise international awareness and understanding of the threat, and this experience taught us two things:

- the threat is evolving fast as the internet increases the exposure of victims whilst offering a ‘safe haven’ for offenders to access imagery and stream live abuse ‘on demand’
- a unified, consistent and cost-effective approach is especially challenging given the collective response draws on a diverse and highly complex stakeholder landscape.

This report deliberately focuses on the online threat – especially the factors that expose children and young people to sexual grooming online, as we believe this is fuelling and facilitating international demand for new abuse images and exposing more victims to harm. At the same time, CSEA requires a multi-modal response and we recognise the vital importance of work by the police, schools, health and social services to protect children in our local communities.

From speaking with experts across the response landscape, we’ve drawn two broad conclusions. First is the opportunity for a small coordinating function – what we’ve described as an ‘Online Harms Safety Centre’ (OHSC) – to orchestrate the collective contributions of every organisation and achieve maximum impact within the most cost-effective system.

“OUR RECOMMENDATIONS SET OUT A PATHWAY TO A POSITIVE HUMAN FUTURE IN A COMPLEX AND CHALLENGING ONLINE ENVIRONMENT”
This would benefit from having industry and third sector organisations ‘inside the tent’, mirroring the success of the National Cyber Security Centre (though keeping the protection of the UK’s cyber infrastructure entirely separate from maintaining citizens’ safety).

Second, we’ve identified that the threat manifests differently on the dark web, the surface web and in the real world, so we’re advocating a tailored response to each with the focus on prevention – targeting offenders and educating potential victims – over traditional measures designed to pursue offenders and protect victims.

We don’t propose replacing other successful organisations like the National Crime Agency’s Child Exploitation Online Protection (NCA-CEOP) unit, part of the Vulnerabilities Command, which works nationally and internationally to bring offenders to justice. Instead, we aim to harmonise NCA-CEOP’s work with the complementary contributions of policy-makers, regulators, industry solutions and third sector insights.

Despite the challenges and our recommended changes, the UK is widely regarded as leading the global approach, with the Economist Intelligence Unit’s CSEA response benchmarking index ranking the UK first internationally for its response to sexual violence against children.

However, those perpetrating CSEA and spreading the imagery are operating in increasingly sophisticated ways. Respondents across the landscape are battling to catch up and keep up. Our recommendations set out a pathway to a positive human future in a complex and challenging online environment.

This would represent an important step towards the ‘whole system approach’ described in the UK Government’s Serious and Organised Crime Strategy, putting the CSEA mission on the same footing as the collective responses to counter-terrorism and cyber security.
Definitions and scope
The UK Government defines CSEA as “a form of child sexual abuse [which] occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology.”

UK Government Publishing Service, 2017

Across this space, we encountered different organisations using different terms to describe the threat, such as Child Sexual Abuse and Exploitation (CSAE). For the sake of consistency, we have continued to use CSEA, the term used in our previous work with the WePROTECT Global Alliance (see page 7).
WE NEED TO RE-THINK THE COLLECTIVE RESPONSE TO ONLINE CSEA

Tougher regulation alone won’t stem the rising tide of online child sexual exploitation and abuse (CSEA). Nor will the demonisation of the so-called ‘technology giants’. While there is a growing and understandable clamour for action to better protect our children online, and a Government pledge to enact new legislation, the sophistication of the threat and complexity of the response landscape calls for a re-think of the way we collectively respond.

In the UK, greater political awareness of the threat, better law enforcement capabilities and strong public feeling have coalesced to support a comparatively robust response, enabled by broad children’s care reforms and investment in innovation and legislation. But despite these positive advances, we’re seeing a significant and worrying growth in the online threat.

For example, through the ‘sextortion’ of teenagers and young people engaged in online social networking. This entails blackmailing children online by convincing or intimidating them to share sexually explicit material, then threatening to share that material more widely as a means of extracting increasingly explicit content. Some cases see victims followed for years, with offenders using social media to stalk and control them. And these children suffer each time these images are shared.

Even the UK’s significant progress in tackling online CSEA pales relative to the scale of the challenge ahead:

- UK police forces have seen a 700 per cent increase in referrals of child abuse imagery since 2013, rising to 82,109 in 2017 – or 6,842 per month
  
- the Internet Watch Foundation (IWF) recorded a 35 per cent increase in child sexual abuse image and videos from 2016 to 2017, rising to 80,318 reports
  
- cases of child sexual offences committed online have tripled (from 3,186 to 9,543) over the past three years
  
- and in the 18 months since sexual communication became an offence in April 2017, the police recorded more than 5,000 online grooming offences.
OUR METHODOLOGY

Last year, the WePROTECT Global Alliance asked us to compile a *Global threat assessment* of online CSEA by speaking to agencies and experts involved in the international response. The research highlighted the disturbing scale of the challenge facing public and private organisations around the world. It concluded that technology is enabling unprecedented levels of offending, with greater levels of organisation, which in turn creates new and persistent threats as these individuals and groups exploit online ‘safe havens’ and ‘on-demand’ access to victims.

Building on this, and with a view to further exploring how to enhance the collective response, we invited key respondents from across the national and international landscape to discuss their role and remit, how they collaborate with other stakeholders (or fail to), successes and challenges, funding and technology, as well as their wider thoughts and insights.

We spoke with senior officials and experts from 16 organisations across the response landscape, from Government, law enforcement, industry and the third sector. Respondents included CEOs, policy leads, directors and research leads from the Home Office, the National Police Chiefs’ Council (NPCC), the National Crime Agency (NCA), the NSPCC, the IWF, Microsoft, Facebook, Twitter and Amazon Web Services. For a full breakdown of respondents, please see page 34.

WePROTECT GLOBAL ALLIANCE

WePROTECT is an international collaboration dedicated to ending online CSEA. As a founding industry member, we’ve helped develop policy, business and technical solutions to support the global fight against child exploitation.

Membership of this single global movement against the sexual exploitation of children online now stands at 82 governments, 20 global technology companies and 24 leading international and non-governmental organisations (NGOs).

Since its inception, the alliance’s partner governments and organisations have built databases and established hotlines to move towards proactive identification and removal of online CSEA material. It’s now taking steps to increase the speed and efficiency of content takedown through automated solutions.
TODAY’S RESPONSE TO CSEA

It’s a complex response landscape. We identified the primary sectors and organisations actively engaged in combating CSEA to show the current alignments between them. Whilst there are strong structural connections between policy staff, law enforcement and intelligence agencies, there is no single front door for public sector interactions with industry and the third sector, nor for industry and the third-sector to seek advice or offer capability to Government departments and agencies.

Our survey interviews focused on the four key segments of this landscape with the strongest connection to tackling online CSEA: government, the law enforcement and intelligence community, the technology industry and the third sector.

Reference:
GOVERNMENT
Both nationally and internationally, their primary focus is on the strategy and policy responses to CSEA and related online harms and security issues.

LAW ENFORCEMENT AND INTELLIGENCE
The NCA-CEOP team coordinates the law enforcement response to child sexual exploitation and abuse, and works closely with police and intelligence agencies in the UK and overseas.

TECHNOLOGY INDUSTRY
This ranges from small-to medium-sized technology companies through to the ‘technology giants’, essentially the hosts of technology platforms and services misused by offenders to carry out online CSEA offences.

THIRD SECTOR
Each element works in close collaboration with civil society organisations like the IWF and the US National Center for Missing and Exploited Children. This sector has diverse roles, including: provision of victim support services; offender rehabilitation; internet monitoring and content removal.

Figure 1: Organisations with whom UK institutions interact most frequently

Source: PA Consulting
HOW TO ENHANCE THE COLLECTIVE RESPONSE TO ONLINE CSEA

Achieving the most effective national response to online CSEA requires a re-think of the way Government, law enforcement, technology companies and third sector organisations collaborate.

Across this complex landscape, we see an opportunity to enhance the way children are protected by improving the response in three environments: the dark web, the surface web and the physical world.

To effectively impact these three environments, our research and experience suggests there should be an Online Harms Safety Centre (OHSC) to orchestrate the collective skills and capacity of organisations across the response landscape, allowing them to play to their areas of expertise as part of a wider view of the end-to-end threat.

Government should create the OHSC but it should sit independently, replicating the models used by the National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI).

It would be quick to establish and adaptive, running on a lean staffing model of central secretariat and seconded experts from across the threat landscape.

However, we’re clear the OHSC should be a separate entity to the NCSC. The threats to our infrastructure and citizens are entirely unique, and better served with separate response functions at this time.

And while our study has focused on the prevention of online CSEA, we believe the OHSC could become the central coordination entity for all activity across the online harms landscape, including preventing extremism, intolerance, self-harm and suicide-related material.

TACKLING THREE THREAT AREAS

We recognise there is a national Serious and Organised Crime (SOC) Strategy setting out law enforcement’s aim to disrupt and pursue offenders, protect the vulnerable, prevent the problem at source and prepare a single, whole system approach. To deliver these objectives and improve the collective response across the landscape, we believe there must be distinct approaches to three unique but interdependent threat environments: the dark web, the surface web and the physical world.

The OHSC would coordinate the response across the three areas of focus, with a mission to:

- **disrupt** the dark web webmasters, around whose services offenders congregate and share ‘tradecraft’, CSEA imagery and hints and tips on evading detection and arrest
- **direct** proportionate and balanced regulation of the surface web, where paedophiles pose as young people to groom potential victims and exploit encrypted services to view and share imagery and ‘on demand’ abuse
- **educate** children in the physical world to better prepare them for online interactions by using preventative real-time technology and encouraging responsible online citizenship.
SURVEY FINDINGS...
COORDINATION IS A KEY CHALLENGE FOR ALL CONTRIBUTORS

Respondents were positive about the advances in public awareness of the threat, improved collaboration between some stakeholder groups and the use of innovative technologies to disrupt offenders.

They felt relatively joined up with other organisations working to tackle online CSEA. Most described productive relationships with at least one key partner and there was general recognition that collaboration with law enforcement in the UK is working well. The perception is that national coordination in the UK is better than what has been achieved internationally.

There’s clear progress towards a national law enforcement strategy. And there’s now a single database of child abuse imagery that all UK police forces and the NCA can access, making it possible to identify images and have them removed more quickly.

But respondents flagged the absence of a coordinated national response to online CSEA across the wider response landscape. This has led to a number of well-intentioned but rival initiatives, overlaps of activity and focus, and a lack of clarity over roles and responsibilities with partner organisations and the wider community.

For example, we’re aware of multiple Government departments having implemented industry engagement roles to address specific threats, with limited coordination between the roles to streamline engagement and prevent overlap and duplication of effort. And while most organisations are seeking ways to work better together, one respondent lamented the “cavalier approach” of some organisations.

While most interviewees understood the specialist contribution of their organisation, they were less clear about where they fit in the bigger picture and how to achieve greater impact. Coordination across the main stakeholder groups is mostly limited to the operational response rather than strategy or policy formulation.

Some respondents described the challenge of competing for funding with other missions (such as counter terrorism), conflicting policy drivers and a lack of cross-Government alignment to maximise the impact of interventions.

Worse still, respondents told us about initiatives and technologies with the potential to play a major role in the response to online CSEA that haven’t been scaled as industry isn’t part of the conversation.

An example of this is the ReThink app, a real-time cyberbullying prevention product that notifies users they might be about to commit online abuse. Such technology could also alert potential victims of online CSEA and deter offenders from accessing criminal material.
Top barriers to greater collaboration with national partners

- Legal or policy constraints
- Funding constraints
- Restricted professional familiarity between practitioners

Top barriers to greater collaboration with international partners

- Differences in international legal or policy positions
- Different cultural perspectives
1. RESPONSIBILITIES AND OPERATIONS

The 2018 National Security Capability Review places the UK’s response to serious and organised crime at the ‘top table’ alongside defence, counter-terrorism, cyber security and national resilience. This is reinforced by the Government’s SOC Strategy, which gives the CSEA mission the full attention of the UK National Security Council. There is a strategic action plan to address the National Security Advisor’s sub-threats of online CSEA, contact child sex abuse and transnational child sex offences.

Whilst the Home Office takes a lead on the Government response to online CSEA, the Department for Digital, Culture, Media & Sport (DCMS) plays a role in framing ‘online harms’ regulation. The Department for Education (DfE) retains the lead for educating children about internet safety. Other ministries, including the Department of Health and Social Care, and the Department for Communities and Local Government, play a vital role within local communities, supporting victims of physical exploitation and abuse. Consequently, the local safeguarding landscape can feel disconnected from the national response.

While Government respondents believed they’re “relatively joined up” with wider stakeholders, one respondent told us: “The challenge is that we don’t know what we don’t know. How do you reach out to someone you don’t know exists?”

Another worry was that “different people are having the same conversation with many people”. This confusion is mirrored in how success is measured, with respondents admitting they use a “mixed bag of indicators” that often focus on outputs rather than outcomes. Government stakeholders also explained the difficulty of establishing clear and realistic expectations with industry.

“THE CHALLENGE IS THAT WE DON’T KNOW WHAT WE DON’T KNOW. HOW DO YOU REACH OUT TO SOMEONE YOU DON’T KNOW EXISTS?”

SURVEY FINDINGS: GOVERNMENT PERSPECTIVES
2. IMPACT OF TECHNOLOGY

Respondents believed industry has taken a “big step forward” on the technology front, with advances such as hashing – a form of digital fingerprints that represents sexual abuse imagery with a code – helping organisations identify and remove CSEA material. Hashing also helps protect those involved in identifying criminal content from having to look at distressing images multiple times.

But it’s “relatively difficult” for the Home Office to keep up with the digital arms race. While the Civil Service is “better off than most”, the prioritisation of “agility and transferable skills rather than deep technical knowledge” means significant upskilling of people is required. Respondents also conceded that Government is “focused on the now rather than investing in the future.”

THE BIGGEST CHALLENGE IS PROMOTING MORE EFFECTIVE COLLABORATION WITH INDUSTRY AND FINDING THE RESOURCES TO MATCH THE THREAT.

3. WIDER LANDSCAPE AND FUTURE PLANS

While national stakeholders are “doing a good job”, it’s “well known now that police are overwhelmed by the scale of reporting” – even before the true scale of offending is understood.

While there is pride in the UK taking the lead on the EU response and international engagements, Government would value an increased focus on cross-border measures. In some cases, victims are in the UK and the perpetrators offshore, along with the internet-based services they use for communicating and sharing child sexual abuse material. In other cases, the offender may be live streaming ‘on demand sexual abuse’ of children located overseas (known as cybersex trafficking) from the UK.

So, the response necessarily involves significant international cooperation and collaboration to safeguard victims, pursue perpetrators, and target the servers and dark web services that host paedophile web forums and transmit abuse imagery.

The biggest challenge is promoting more effective collaboration with industry and finding the resources to match the threat. One official told us: “Industry often sees their role as more to ensure that anything that appears on services or platforms is removed... [We] would advocate or push for a more proactive role in ensuring that it doesn’t happen in the first place.”

However, better collaborative working has been evident in the way the Home Office and DCMS have consulted widely with tech companies, children’s charities and other stakeholders to set out legislation in the Online Harms White Paper.
SURVEY FINDINGS:
LAW ENFORCEMENT AND INTELLIGENCE PERSPECTIVES

1. RESPONSIBILITIES AND OPERATIONS

Law enforcement roles range from local interventions against individual abusers to the use of advanced capabilities in pursuit of technically sophisticated offender communities. In the UK, the law enforcement response is led by the NCA’s Child Exploitation Online Protection (NCA-CEOP) unit, supported by specialist technical capabilities drawn from GCHQ (Government Communications Headquarters).

Since 2014, GCHQ has a publicly avowed role to combine their technical skills with the investigatory expertise of NCA officers to crack down on paedophiles operating on the dark web, whilst Chief Constable Simon Bailey provides policing leadership for child protection on behalf of the NPCC.6

This NPCC/NCA-CEOP/GCHQ response is widely regarded as an international exemplar that other countries are mirroring, such as the Australian Federal Police. Coordinated UK activity sees the arrest of over 400 offenders each month and more than 500 children safeguarded, which represents a 12-fold increase over the past decade.7

Much of law enforcement’s online CSEA work takes place in conjunction with other Government bodies such as the Home Office, although respondents say there’s a lack of clarity around areas of focus. Given the wide range of departments tackling different aspects of online harms, from extremism and ‘hate speech’ to self-harm, cyberbullying and revenge pornography, a joined up approach across industry is lacking and all interviewees indicated resourcing issues.

There has been significant progress developing national strategies, governance and operating models. For example, the recent national SOC Strategy sets out specific commitments for tackling CSEA, with four objectives: to disrupt and pursue offenders, protect the vulnerable, prevent the problem at source and prepare a single, whole system approach.

Our interviewees indicated the ‘why’ and ‘what’ of these strategies are clear, but clarity on the ‘how’ has not yet trickled down beyond senior Government and law enforcement circles. Nevertheless, this needs to be viewed in the context of the Economist Intelligence Unit’s CSEA response benchmarking index scoring the UK 100/100 for national plans and policies.8
Since 2014, all UK police forces and the NCA have connected to the Child Abuse Image Database (CAID), which contains more than 10 million indecent images of children and 30 million hashes. This gives investigators better tools to search seized devices for indecent images, accelerates the identification of ‘known bad’ images and improves victim identification. In 2017/18, UK law enforcement agencies identified 664 victims within indecent images of children, compared with 177 in 2014/15.\(^1\)

The biggest challenge for law enforcement is keeping pace with rapidly changing technology, particularly given funding pressures. “Our adversaries are technologically aware and therefore there is a requirement for a significant uplift in capability,” one interviewee revealed.

Our respondents were keen to build trust with wider industry to enable a more collaborative response, with one stating we must “get technologists together to create solutions”.

Another key focus was on having the right people with the right skills. “Everything flows from that,” one respondent indicated.

Despite the unique multidisciplinary work of NCA-CEOP and its engagement with the NPCC, industry, NGOs and policy officials, respondents still wanted to see better collaboration across the board. Their responses indicated a better coordinated strategy to engage academia and business could greatly reduce the overall risk picture. Rather than law enforcement taking ownership of projects, interviewees suggested this could be better facilitated through more collaborative relationships.

The future of online CSEA operations across Government and law enforcement rests on creating a more balanced and aligned approach to improve coherence. According to interviewees, this needs to include:

- a streamlined approach to funding
- a more integrated operating model, especially with industry and the third sector
- better resource allocation
- recognition of technical requirements to keep pace in the digital arms race
- stronger engagement with industry and a wider community of interest around clearly defined objectives.
1. RESPONSIBILITIES AND OPERATIONS

The tech industry goes beyond the ‘web giants’ and also encompasses application service providers (e-mail and chat services, and social media platforms) and other players of all sizes with a role in promoting online safety.

Our respondents predominantly saw their role as supporting law enforcement by flagging and reporting suspicious content and activity, as well as “putting technology in the hands of those that need it”. While cognisant of their responsibility to be at the forefront of tackling online CSEA, they believed efforts would be better spent on root cause interventions rather than the enabling technology. Although their own roles and responsibilities are “very clear” to them, the requirements for network and application service providers to collaborate across industry is loosely defined. One respondent told us: “We are not working collaboratively... the whole is less than the sum of the parts.”

Success is currently measured in three ways:
- the speed of detection and reporting of offensive material
- law enforcement feedback on the quality of reporting
- statistics on the volume of data identified and removed before being reported by customers.

The organisations also value feedback about follow-on arrests and convictions, with one respondent saying it helps human moderators “know that their work is meaningful” – particularly as “reviewing this type of content on a constant basis takes a toll”.

“WE ARE NOT WORKING COLLABORATIVELY... THE WHOLE IS LESS THAN THE SUM OF THE PARTS”
2. IMPACT OF TECHNOLOGY

Respondents told us how improvements in digital technologies have enabled offenders and offender communities, providing them with unprecedented levels of access, new capabilities and increasing confidence to abuse children on a mass scale. Technology provides the ability for criminals to seek likeminded individuals while masking their identity. Our respondents acknowledged technology’s role as an enabler for online harms and would welcome Government direction on responding to this threat.

But technology is also helping respond to the challenge. For example, 97 per cent of the online CSEA images removed by Twitter in its last reporting period (Jan to Jun 2018) were flagged by a combination of internal tools and technology, including PhotoDNA – which identifies content similar to that already flagged as criminal.9

One tech firm told us they see their role as reducing barriers so law enforcement can better use AI and machine learning. Another said they wish there was more technology could do to prevent material being created or viewed, rather than being used reactively.

Tech firms are constantly having to innovate to keep up with what one tech player called “a cat and mouse game” with criminals. These firms need to be able to cope with the volume of data and detect real-time crimes on private communications and live-streaming services. Respondents told us the focus on tech “will only work if we add in the missing parts” – people, processes, policies and information.

3. WIDER LANDSCAPE AND FUTURE PLANS

Our interviewees believed that while technology firms are wholeheartedly engaged in this fight – encouraged by the shift from an adversarial approach towards Government providing better information to help combat the problem – the full potential of collaboration is yet to be realised.

Government, law enforcement and industry must keep working together to openly share technologies and methodologies across platforms nationally and internationally. One respondent told us: “Only some countries are beginning to take the CSEA threat seriously due to cultural differences, and so gaining global consistency of approach would help.”

“ONLY SOME COUNTRIES ARE BEGINNING TO TAKE THE CSEA THREAT SERIOUSLY... SO GAINING GLOBAL CONSISTENCY OF APPROACH WOULD HELP”
SURVEY FINDINGS

THIRD SECTOR PERSPECTIVES

1. RESPONSIBILITIES AND OPERATIONS

Clarity on the individual contribution and expertise of third sector organisations, and how they can best work together, is mixed. Respondents told us their roles include the removal of indecent material, research and policy development, Government and industry engagement, and supporting victims and those at risk.

One told us that, while Government provides “great leadership” from the top, “there is a need for a collaborative approach and developing interventions together with Government, policy, law enforcement, NGOs and industry.”

With notable exceptions – such as the WePROTECT Global Alliance – there’s a lack of international strategy or collaboration and some felt the UK should seize this as an opportunity to lead.

The sector regards the prevention of online CSEA as the most significant measure of success, although the lack of a feedback loop means there’s no consistent method of measuring the number of victims safeguarded.

Several respondents expressed the view that industry has the resources and capability to do more but has been unwilling to be transparent on either their work or approach to making online platforms safer. They hoped industry would become increasingly willing to work with the third sector and become a “critical friend”.

“A GOOD Regulatory outcome would need to be a cultural shift... going beyond compliance into a culture of safety”
2. IMPACT OF TECHNOLOGY

Technology is considered a “significant enabler” of offending, with anonymity tools and increased offender sophistication cited as key challenges. Victims are increasingly and unwittingly exposed.

But respondents were keen to stress that demonisation of the technology giants isn’t helpful. “There is a danger that sledgehammer legislation is enforced,” one organisation told us, adding that more can be achieved through open, trusting conversation and bringing in a wider range of partners such as online games designers – an alternative avenue where offenders can groom children. Another respondent added: “A good regulatory outcome would therefore need to be a cultural shift, achieving not only compliance but going beyond compliance into a culture of safety.”

There are differing views on how technology can help respond to the challenge. One organisation told us it helps to be able to stay one step ahead, but others conceded they struggle to keep pace with offenders. Those working directly in safeguarding and victim support don’t feel technology helps them.

3. WIDER LANDSCAPE AND FUTURE PLANS

While third sector organisations were all keen to see increased collaboration and more clearly outlined roles and responsibilities, the major ambition is to raise a generation of children who are educated about the risks.

The challenge is to achieve this against an “exponential” increase in the threat and dwindling resources for prevention and victim support. One respondent told us: “No one knows precisely how much content is out there and therefore the true scale of the issue remains unknown.”

Third sector organisations also told us there can be a “David and Goliath” effect when they attempt to interact with large technology firms. To overcome the differences in ways of working and different speeds of work, our respondents wish to see key actors from across the landscape brought together in a single collaborative forum.
Recommendations...
TACKLING CSEA REQUIRES AN ORCHESTRATED RESPONSE

While the collective resources and expertise of organisations across the landscape offers broad coverage against the online CSEA menace, the complexity of the threat and its rapidly evolving nature means the UK needs a better orchestrated approach across Government, law enforcement, technology companies and third sector organisations.

An Online Harms Safety Centre (OHSC) should be established to enhance the current online CSEA response and create a single point of coordination for the agencies involved. Just as the Government created the NCSC to provide a neutral, unified source of advice and guidance on cyber security, it should also set up an OHSC before transitioning it to operate as an independent entity.

The OHSC model would provide the coherence currently lacking - leading to the creation of a unified enterprise that is greater than the sum of its parts.

Government respondents expressed reservations about the cost and complexity of establishing another enterprise on the scale of the NCSC or the CPNI. However, we believe the OHSC could operate on a lean staffing model based on a small Government secretariat team with seconded experts from law enforcement, the technology industry and the third sector.

A similar approach is used by the UK military’s Permanent Joint Headquarters (PJHQ), which orchestrates integrated military operations without direct control or ownership of the platforms or personnel deployed. These are retained by the Navy, Army and Air Force, with each operating as either the supported or supporting element for each contingency.

Creating a ‘single point of truth’, the OHSC would:

- provide a central, consistent view of respective organisational roles and responsibilities
- identify and mitigate duplication, and support better alignment of funding
- remove the need for new participants to spend time and resources understanding and navigating the landscape
- create a consistent public narrative on the online CSEA threat and response
- encourage greater collaboration with small- and medium-sized enterprises, many of which already own solutions that are unused, whether due to a lack of visibility or the investment required to scale them more widely.

The OHSC would not own and control activity. Instead, its holistic view of the landscape would allow those already working in this space to collectively achieve a more efficient, economical and successful response.

Nor would the OHSC hold the collective purse strings. Rather, it would act as the conduit for central Government funding, enabling better cost effectiveness and increased accountability.

Such a model would let the Government create it as soon as possible and ensure it’s adaptive by nature – both key features when tackling a rapidly-evolving threat. Rather than this being additional cost, it will free up resources by removing duplication of effort – as well as providing a single conduit for discussions, ideas and greater collaboration.

In both its structure and in carrying out its role, the OHSC would need to ensure its functions and any services it contracts out to others are discharged with full regard of the need to safeguard and promote the welfare of children, in accordance with Section 11 of the Children Act 2004.10
The Longer-Term View

Cognisant of the rapidly evolving nature of the threat and persistent budgetary constraints, the OHSC would offer a practical and sustainable means of enhancing the response to online CSEA in the immediate future.

Over the longer term, we envisage closer alignment between the OHSC and the NCSC – with coordinated oversight of how we protect both the UK’s digital infrastructure and our citizens from online harms.

However, the threats to our infrastructure and our citizens are so different and evolving at such pace that we believe they’re better served with separate response functions at this point in time.

Our society’s social web culture and the global proliferation of high speed, low cost internet access has created a unique threat. It’s only as our understanding grows that a combined focus on infrastructure and online citizen security could sit as two divisions of the same entity.

And whilst our analysis is focused on online CSEA, we believe our recommended approach could eventually be extended across other online harms impacting the public.
**RECOMMENDATIONS:**

**ADOPT A TAILORED APPROACH TO THE THREE TIERS OF THREAT**

We believe the online CSEA environment is currently misrepresented as a single entity, with a simplistic (and adversarial) narrative that emphasises the need for the ‘web giants’ to proactively detect and remove harmful content from their platforms.

Through our interviews and work in this area, we have identified three distinct ‘threat environments’, each of which requires a unique and tailored response:

- **the dark web**, which has enabled new safe havens online for offender communities to share, discuss and plan coordinated CSEA offences

- **the surface web**, where offenders groom children online, share images and stream live child abuse

- **the physical world**, where contact abuse occurs (and from where children’s exposure transitions from real world to online harms).

We estimate that most of the effort and resources are targeted at regulating the surface web, with a growing awareness (but small response) targeted at the dark web and very limited investment in using technology to alert children to online risks. The focus of the OHSC would be organised according to these three threat environments, with the following objectives:

- **disrupt** the dark web webmasters, around whose services offenders congregate and share ‘tradecraft’, CSEA imagery and hints and tips on evading detection and arrest

- **direct** proportionate and balanced regulation of the surface web, where paedophiles pose as young people to groom potential victims and exploit encrypted services to view and share imagery and ‘on demand’ abuse

- **educate** children and better prepare them for online interactions using preventative real-time technology and encouraging responsible online citizenship.
RESPONDING TO THREE THREAT ENVIRONMENTS

Each threat environment requires a distinct approach that draws upon specialist response capabilities. The OHSC would orchestrate the approach to each environment and the end-to-end response, enabling better oversight of areas of overlap. For instance, as subjects escalate up the ‘offender pathway’ from online legal pornography to CSEA material, they’re drawn into dark web worlds where criminal networks offer anonymity and access to more content. These sites often require users to contribute new images as their ‘fee’, which drives paedophiles back to the surface web to groom more victims, fuelling physical world offending.

...the large-scale criminal orchestration of online CSEA

...proportionate and balanced regulation

...and equip children with better information to mitigate online risks

THE SINGULAR AND COLLECTIVE THREAT ENVIRONMENTS WOULD BE ORCHESTRATED BY THE OHSC

Figure 2: Tackling online CSEA needs an integrated response targeting three areas
RECOMMENDATIONS:

DISRUPT THE LARGE-SCALE CRIMINAL ORCHESTRATION OF CSEA ON THE DARK WEB

Online offenders operate globally, making it impossible for local legislation and disparate deployment measures to tackle the threat. A technically sophisticated and coordinated law enforcement approach is required in response to the guile of offenders operating within the vast virtual infrastructures of the dark web.

While physical crimes need a local response to pursuing offenders and supporting victims, the online threat is unconstrained by regional or even national boundaries. This has led to instances where UK-based victims are targeted by perpetrators who are based offshore, along with the internet-based services they use to share imagery. In other cases, UK-based offenders may live-stream the abuse of children overseas.

The response requires an unprecedented level of international co-operation and collaboration to safeguard the victims, pursue the perpetrators, and target the servers and services that host and transmit abuse imagery and paedophile web forums. No one agency can tackle this alone. Advanced dark web disruption strategies are expensive to develop and apply, and their long-term success relies on a consistent and coordinated response.

UK and US intelligence agencies are leading the way in the development of advanced technical capabilities to overcome these challenges, which also impact international terrorism, extremism, espionage and other serious organised crimes. They’re uniquely placed to identify tactics and approaches to tackle online CSEA by re-purposing techniques developed for other missions. Examples include the use of AI on video-sharing platforms that automatically recognises terrorist propaganda and behaviours that may indicate extremist activity.

Together with organisations like Europol and Interpol, intelligence agencies – working in close partnership with NCA-CEOP – are core components of a maturing global alliance. With continued investment and coordinated collaboration, this partnership has the collective capability to sustain the relentless disruption of dark web services used by offender communities and international organised crime groups.

Given the technical complexity and operational sophistication of the criminal enterprises behind these dark web forums, combined with the scarcity of advanced cyber skills across Government, this is the area where GCHQ’s high-value expertise and resources should be focused.
WHAT IS THE DARK WEB?

The dark web is the part of the internet undiscoverable by normal means. Accessing its content takes specific software, configurations or authorisation.

It operates under the radar of law enforcement and search engines, and requires an anonymising browser to be accessed. It hosts a range of networks, from small peer-to-peer ones to popular encrypted ones like Tor, which claims to have two million users every day.\textsuperscript{11}

There are dark web sites dedicated to various aspects of CSEA offending. Many have tens or hundreds of thousands of registered members. The US Department of Justice reports that an aggregate 1.9 million users are registered across nine sites dedicated to this material.\textsuperscript{12}
RECOMMENDATIONS:
DIRECT PROPORTIONATE AND BALANCED REGULATION OF THE SURFACE WEB

On 8 April, the UK Government published its Online Harms White Paper, which commits to a new regulatory framework to improve citizens' online safety. It clearly places online CSEA harm on a par with terrorist material designed to spread propaganda and radicalise as the most serious forms of illegal content and activity. It also identifies other harmful effects of online disinformation, social media promotion of gang culture to incite violence, and the use of the internet to harass, bully or intimidate, or to expose vulnerable adults and children to harmful content such as self-harm and suicide.

We welcome the prioritisation of online CSEA but note this mission has not yet achieved the equivalent level of organisational maturity as the UK's strategic responses to countering terrorism and maintaining cyber security. The internet giants have been unable to control the sharing of child sexual abuse imagery and its associated tradecraft for too long.

They have no appetite to be the moral arbiters for what should and shouldn’t be on the web, or to establish the precedent of liability for policing the online world, and no responsible government should put such a responsibility in their hands.

Our conversations with stakeholders across the landscape suggests they would, however, welcome a principles-based, proportionate regulatory environment that addresses online harms – recognising that industry needs to keep improving and do more. For example, Facebook CEO and co-founder Mark Zuckerberg called for common rules that all social media sites must abide by, enforced by third party bodies, and a common global framework to ensure laws are standardised globally.13

A new regulatory body can sharpen and focus industry and international engagement. But regulation will hinder efforts if it deploys a sledgehammer response to this nuanced and evolving threat.

When setting up regulators, we’ve found that smart, effective regulation occurs when the body has the power to enforce but is also a champion of industry, working to ensure regulation is proportionate and balanced, builds on existing good practice, and protects free speech. The regulatory body must also have the agility to respond to a landscape where the threat – and the response to it – is constantly changing, and a clearly defined scope and purpose to ensure its work is joined up and coherent.

Any regulatory response must also be robust and flexible enough to respond to the use of encrypted apps such as Discord and Telegram, where criminals can exploit the user privacy features to share and discuss abuse.

Informed by the OHSC, but independent of it, this new regulatory body would be equipped with the technical expertise – via advisory panels, seconded support and/or in-house experts – to design effective regulatory frameworks.

The NSPCC’s recent report, Taming the Wild West Web, drew on our regulatory research to affirm that a stronger sense of regulatory predictability and certainty can support innovation, build awareness and trust. Furthermore, parents and citizens feel better informed and more protected when they’ve heard of the regulator and when any breaches are publicised.14

This new body would draw on a wide network of key collaborators, including the Home Office, DCMS, DfE, technology companies, NGOs and inter-governmental organisations, and the WePROTECT Global Alliance.
The UK is seen as a leader in the international fight against online CSEA, with the Australian Federal Police seeking to mirror the UK’s law enforcement response. There are opportunities for the UK to maintain and improve its wider response through studying other approaches - such as the Australian regulatory approach.

As the UK Government consults on the design of the new regulatory framework and non-legislative package, we believe there are clear lessons to be learned from Australia’s eSafety Commissioner, which established a world-first complaints system for serious cyberbullying of Australian children and has since expanded its remit to cover enhancing online safety for all citizens. The eSafety Commissioner ensures the removal of the most extreme online content whilst providing users with a means of requesting the removal of potentially harmful material, avoiding aggressive regulatory measures. Users and social media firms have positively received these initiatives.

The Australian regulatory model features a robust classification model and a legislated sanctions regime to ensure that Australia does not become a safe harbour for prohibited online content. Under this approach, the eSafety Commissioner can direct Australian CSPs to remove content from their services through takedown notices, service-cessation notices and link-deletion notices. These prohibitions are backed by strong sanctions for non-compliance, including civil penalties. To date, there has been 100 per cent compliance with takedown notices from the Australian Internet industry.
**RECOMMENDATIONS:**

**EDUCATE CHILDREN TO ENHANCE ONLINE CSEA PREVENTION**

With the current rate of offending threatening to overwhelm police, the long-term prevention strategy must focus on educating children and their adult influencers so they are equipped to minimise the threat they face – just as the Green Cross Code was implemented to tackle the growing issue of pedestrian fatalities and injuries in the late 1960s.

It’s no longer enough for companies to hide online safety information in terms and conditions on a corporate website. Nor can we expect parents to adequately monitor their children’s online interactions – teenagers can all too easily bypass monitoring software or refuse to engage with apps that allocate control to adults.

Real-time education technology can play a key role in minimising the threat of ‘sextortion’, where groomers convince or intimidate teenagers and young adults to share sexually explicit material, and then threaten to share that material to obtain increasingly explicit content.

In the same way that banks and credit card companies alert customers when they suspect fraudulent transactions, we believe the same AI technology should be used to send children (or vulnerable adults) automated alerts when dangers are detected in their online chats, preventing the crime from taking place. AI can look for and flag suspicious indicators, including language traits and the use of anonymising techniques.

This technology is already in use in the form of the ReThink app, cyberbullying technology that gives users the opportunity to pause and reconsider before sending messages, and which has been proven to reduce the occurrence of online abuse through real-time education.

We believe social media companies should voluntarily adopt the use of in-app technology to offer children real-time, relevant risk information that will help a whole generation build their digital resilience. While the implementation of the technology may vary, we’ve developed a set of principles that should apply to all real-time prevention technologies.

**PREVENTION THROUGH SELF-EDUCATION**

As well as the ReThink app, other innovative examples of educational approaches to internet positivity and responsible citizenship include the IWF’s ‘So Socking Simple’ campaign, which highlights the importance and simplicity of reporting sexual images where those involved may be under 18.

Other examples include the NSPCC’s ‘talk PANTS’ campaign, which teaches children how to stay safe from abuse via apps and school resources, and the NCA’s Jessie & Friends series, which uses animated videos and resource packs to equip 4- to 7-year olds with the knowledge, skills and confidence to stay safe online.
Our Five Principles of Online Safety Alerts

<table>
<thead>
<tr>
<th>Instant</th>
<th>Specific</th>
<th>Relevant</th>
<th>Private</th>
<th>Supportive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts should be shown in situ as soon as the risk is detected, e.g. a chat bubble.</td>
<td>General warning alerts and notifications are ignored. Alerts must relate to the user, their situation and their current chat.</td>
<td>Alerts must be in the same style as the rest of the online experience – avoiding any risk of being ignored and avoiding alert fatigue.</td>
<td>Children must be trusted to do the right thing with the right information. Alerts should be separate from law enforcement activity but don’t excuse tech firms from legal reporting requirements.</td>
<td>Online risk is complex, so links should be included to where more information can be found, or towards people who can help.</td>
</tr>
</tbody>
</table>

Some law enforcement respondents suggested any in-app technology should always alert them in the first instance to online grooming, while third sector respondents believed that parents or carers should be notified. Our belief, based on extensive research in this area, is these principles should be a digital equivalent of the Green Cross Code, empowering and equipping children to understand the risks and choose the right course of action through a focus on education and prevention.

It’s time for a completely new approach to the way we educate children about online dangers. Guided by these principles and harnessing existing technologies, we believe the OHSC can convene groups across law enforcement, Government, the third sector and technology companies to oversee a coherent offline and online educational strategy for children. And this should be supplemented by a relentless focus on intervention and support.
About the survey

In late 2018, PA commissioned a survey of senior representatives from Government, law enforcement organisations, the technology industry and third sector organisations to help improve understanding of the collective responses to online CSEA.

The purpose was to identify the stakeholder landscape collectively tackling online CSEA and explore whether these organisations believe there’s a need to drive closer joint working and co-operation, and whether there are opportunities to drive a more effective and integrated response.

This survey covered five areas:
- each organisation’s roles and responsibilities
- day-to-day operations
- impact of technology
- wider landscape
- future plans.

Representatives of the following 16 organisations participated in the survey that informed this report, either in face-to-face interviews using a standard survey questionnaire or in writing. As many of the respondents hold operational law enforcement roles or are actively engaged in the operational response to combatting online CSEA, individuals are not named to protect their privacy and security:

- WePROTECT Global Alliance Secretariat
- Home Office (Tackling Exploitation and Abuse Unit)
- NPCC (Child Protection)
- NCA-CEOP
- Government agency: Serious and Organised Crime Team
- Anglia Ruskin University (Policing Institute for the Eastern Region (PIER))
- NSPCC
- Barnardo’s
- The Children’s Society
- IWF
- eSafety Commissioner (Australia)
- Microsoft
- Facebook
- Twitter
- Amazon Web Services
- Crisp Thinking

Endnotes:
1. Global threat assessment 2018 by WePROTECT Global Alliance and PA, published October 2018
2. Annual Plan 2018-19 by the National Crime Agency, published April 2018
3. Annual Report by the Internet Watch Foundation, published April 2018
5. Over 5,000 online grooming offences recorded in 18 months, NSPCC, published March 2019
6. PM announces new global action to deal with online child abuse by GOV.UK, published December 2014
7. Four-year-olds taught for the first time about online dangers as threat increases by National Crime Agency, published March 2019
8. Out of the shadows by the Economist Intelligence Unit, published January 2019
9. Evolving our Twitter Transparency Report by Twitter, published December 2018
11. Users by Tor, accurate as of April 2019
12. US Department of Justice, January 2018
13. Mark Zuckerberg asks governments to help control internet content by BBC News, published March 2019
14. Taming the Wild West Web by the NSPCC, published February 2019
Authors

Report authored by our defence and security experts

Nick Newman
Nick leads PA’s work with the UK homeland security clients and has spent the past decade working with the security, law enforcement and criminal justice communities to tackle their most critical challenges: helping to detect, prevent and disrupt crime, protect the public and save lives. Nick has helped develop policy, business and technical solutions to support the global fight against child exploitation and led PA’s involvement as one of the founding members of the WePROTECT Global Alliance.

Graham Lovell
Graham works with policing and security clients to help them solve complex challenges across both business and technology. Over the last five years, Graham has supported PA’s work to identify ways to tackle online CSEA.

Clare Fraser
Clare has over four years’ experience working on transformational change programmes with security clients across government, bringing together skills in business design and capability building to design and embed sustainable change. Clare is working on the design of operating manuals and a training strategy for the Home Office’s Office for Security and Counter-Terrorism Disistence and Disengagement Programme.

Natalia Greene
Natalia works with policing and security clients to help transform public service delivery and the response to priority threats, including CSEA. Through her time at PA, Natalia has helped to develop innovative operating models to deliver complex change for a range of government clients. Currently, Natalia is working on a UK-led Rule of Law Initiative.

Matt Lindsay
Matt uses his technical consulting expertise to help policing and security clients use technology to achieve outcomes. Matt has a passion for helping the most vulnerable people in society and has dedicated his career to protecting others. Notably, Matt led the technical proof of concept for the WePROTECT Global Alliance system for detecting and providing real-time alerts to protect vulnerable people in online chat apps.

GET IN TOUCH
Contact the team to discuss our research, recommendations and how we can enhance the collective response to online CSEA.

UK: +44 (0)20 7333 616
Email: nick.newman@paconsulting.com
About PA.

An innovation and transformation consultancy, we believe in the power of ingenuity to build a positive human future in a technology-driven world.

As strategies, technologies and innovation collide, we create opportunity from complexity.

Our diverse teams of experts combine innovative thinking and breakthrough technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

We are over 2,700 specialists in consumer, defence and security, energy and utilities, financial services, government, healthcare, life sciences, manufacturing, and transport, travel and logistics. And we operate globally from offices across the Americas, Europe, the Nordics and the Gulf.

PA. Bringing Ingenuity to Life.