Our Strategic Response

International cooperation

The commitment to look at the international nature of online abuse is laudable and we welcome it. However, there are concerns regarding the feasibility of this goal for a variety of reasons.

BCS agrees with the commitment of the strategy to collaborate with international partners. That said, we feel the strategy did not give a significant level of detail as to how this would be achieved. Undoubtedly, the UK ought to use our world-leading position in digital technology and wider international influence to help forge a safer online world. There will, however, be limitations to the extent to which this can work when it is likely that many countries will be unwilling to operate under the same standards as we do. Having a realistic appraisal of the cultural differences between countries and a sense of realism over goals will produce more tangible results as we engage with others.

Given the scale of start-up communities which are outside of any formal control, in addition to the numerous countries producing online content, imposing a consistent set of standards will prove a difficult task. While the strategy argues that the design stage is the best time in which to inculcate safety standards, consistently doing so domestically, let alone internationally, would be difficult from a logistical standpoint. There is a need for both clarity when it comes to the regulatory authority responsible for upholding standards and a defined structure as to how this authority would be able to deal with the vast amount of online content being created and monitored.

Outside of start-ups, there are also likely to be problems in getting major tech firms on board with the aims of the strategy in a timely fashion, especially when action will often not be in their direct economic interest. Furthermore, having major companies on board will often require multilateral action due to their global reach and this will hit some of the aforementioned roadblocks on working across borders. There is a greater degree of confidence around the potential for this sort of action on issues that can be tackled unilaterally, though many online threats are ultimately not national problems.

Individual rights and safety

BCS would highlight the importance between online safety and the right for people to have their privacy protected. Shoring-up the online rights of citizens in a proactive manner must be done concurrently with the strategy. It is reassuring to see that this has been acted upon with the launch of the Data Protection Bill.

The Government made reference to striking the right balance between safety and innovation within the strategy, it is hoped that a similar balance between safety and online privacy can be made too and enshrined within the strategy following this consultation.

Working with industry to make online environments safer for all users

Social media companies and the proposed social media levy

BCS has concerns about whether a regulatory model and levy based on that which is used for the gambling industry was appropriate in relation to social media companies. While a degree of consensus seems to be forming in relation to the roles and responsibilities that industry (in this case social media organisations) must necessarily play to bolster awareness and preventative action, a similar consensus does not exist for a levy.

One reason is the multifaceted nature of how to tackle internet harms and those who have been effected by them, as compared to gambling. Whereas the money being given by gambling companies to GambleAware has an obvious purpose in raising awareness and tackling problem gambling, the same cannot be said for social media. There is also a lack of definition as to what constitutes problem social media usage as opposed to problem gambling. The negative connotations of social media can take numerous forms and more work would need to be done in defining exactly what these are. This would help shape the equivalent version of GambleAware for this sector.

A further potential issue of this approach exists in relation to the independence that such an organisation would have from social media companies, when it would be funded by them. While getting companies to pay to raise awareness of safety issues is an understandable approach from a financial and ethical stand point, it could potentially cause a conflict of interest and more specific information on how to keep such an organisation at arms-length from social media companies would be welcomed. One suggestion might be to commission independent research as to the links between social media and harm prior to setting up such a body, so that any initial stage would be done on grounds that were academically rigorous and not predominantly based on the advice of social media companies.

The question as to what type of companies would pay into the social media levy is explored in the formal DCMS consultation, but BCS largely follows the Government's position that whatever the threshold for contribution, it must not incumber smaller companies, particularly start-ups. There is also a potential issue not mentioned in the strategy around social media companies that are entirely based overseas, but who have large numbers of users in the UK. Sina Weibo, the Chinese microblogging site, currently has a larger worldwide market-share than Twitter, including large numbers of UK users[1]. Despite this, it is far from clear that an organisation such as this would willingly contribute towards a social media levy in the UK, despite being a platform of a significant size and influence.

Another suggestion might be for there to be a permanent forum, or regular meeting, for the major social media organisations to come together and discuss challenges around online harm and threats. While the Government and other groups, including BCS, have already instigated such meetings at various points, they are not regular and often come as a reaction to negative events, such as the online abuse of politicians during the 2017 General Election. Taking a proactive approach to facing down

[1] http://www.bbc.co.uk/news/technology-39947442

online abuse and threats could help to prevent additional problems from developing and encourage greater collaboration between the most ubiquitous social media companies.

Voluntary action

The Government's willingness to leave the door open to statutory action if voluntary provisions were not acted upon by industry is encouraging, though obviously it is hoped that it would not be necessary. If law were to change in order to create a penalty for companies that did not remove hate speech in an appropriate period of time, the penalty must be of a sufficient level to enforce compliance.

The model mentioned by multiple respondents was the German 'Enforcement on Social Networks' legislation from earlier in the year, which enshrines the need for social media companies to remove hate speech within 24 hours in a straightforward case and seven days when the evaluation of content is more complex[2]. The penalties for failure to comply are up to €50 million in this case, though the size of the fine is contingent on the size of the organisation in question.

Ultimately, the strategy will only be a success if all relevant stakeholders have buy-in. While this is not impossible, significant collaborative work will need to be continued between the Government and industry during both the development and implementation of the strategy. The potential for further formal legislation is a reasonable way of encouraging this sort of buy-in.

How can technology improve online safety for all users

Improved technology and improved education

BCS feels the strategy did not focus enough on the role of digital education in reducing harm, as compared to utilising new technology. As a society, we need to do more to educate everyone as we enter the digital age. There is a danger of the strategy being too technologically deterministic and instead; it should also encompass more policies that are not overly reliant on technology or companies changing. Information about safety online ought not to be limited to just those who appear to be vulnerable, like the young and the elderly, and must be in place across for all.

This could potentially take the form of the public-awareness campaigns similar to those place for drinking and driving for example. Potentially, the infrastructure for this is already partially established through the Government's Cyber Aware campaign[3]. An expansion of the programme to cover online abuse and threats, while retaining information about cyber security and crime, could be the basis for getting information to people not in formal education.

The Action Plan for Older People is an encouraging policy within the strategy that runs in contrast to many of the proposals that focus on the young. However, the plan on its own is not enough to deal with the range of online abuses that predominantly effect the elderly. One example is the potential for older people to suffer financial abuse through online dating apps, which has not been considered

[2] https://techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/
[3] https://www.cyberaware.gov.uk/

in depth. Like a variety of proposals suggested in the strategy, the ethos of the plan is welcome, but more detail and depth will be necessary to fully tackle the relevant issue.

A 'safety-first' approach to design

The idea of a 'think safety first' approach, where designers are encouraged to share best practice and both promote and develop guidance to ensure high standards, is to be welcomed. To implement such an approach will be a challenge and it is unclear even with collaboration with organisations such as Tech City UK how much start-up communities can realistically be expected to conform with standards, especially if they are not in the statute books.

The difficulty in the challenge ought not to preclude working towards it. Research shows that the most popular platforms amongst children tend not to be services designed primarily for children[4]. As the online environment has matured and children have become increasingly prevalent users, services have often had to retrofit to create a suitable platform for young people, often in a manner which is against their commercial interest.

Ultimately, having the right starting points for meaningful and implementable design standards is of enormous importance. For voluntary frameworks to work, the Government will need to spread the net far and wide for partners, both to help craft standards that are applicable across industry and to foster an increasing sense of responsibility. This could, in the longer term, provide the basis for regulation.

Supporting children, parents and carers

Teaching digital resilience

The focus of the strategy in terms of children largely rests on protecting them from overt harms, such as abuse or age-inappropriate content and empowering them to make the most of the digital world which they are growing up in. Both aims seem well-intentioned and sensible. A further area which should not be ignored during this process is strengthening digital education for young people in order to increase their ability to be resilient in the online world, even when not being faced by specific online threats.

It is reassuring to see the Government's commitment in the strategy to continuing to offer education about digital resilience through PHSE and RSE. However, a greater degree of original thinking about improved education in the strategy would be welcome and would complement the other parts of the strategy on preventing harms.

Realistically, there are limitations to what can be done with improved design and these gaps are where education is vital. BCS has previously done work on some of the challenges that need to be addressed to allow children to thrive in the digital age. These have included working with the PEEL Project, which explores the self-identity of young people growing up in a world rife with social media and other digital

[4] https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/childrens-media-lives

pressures[5]. It is not just a question of technical skills, having the ability to navigate the digital environment with a strong sense self esteem and ability to think critically is integral to getting the best out of the digital environment.

As a result, more could be done to improve digital education and resilience. The work of BCS through PEEL has previously argued that young people need to have knowledge, understanding of competencies and an appreciation of consequences around the digital sphere. It would be an encouraging development if this was reflected within the strategy to a greater level following the consultation period.

Digital rights for young people

Another proactive approach to helping young people in the digital world is updating and strengthening digital rights. As mentioned earlier in this paper mitigating risks is key, but empowering people online is equally important. BCS has argued that rights already exist through the United Nations Convention on the Rights of the Child (UNCRC) that could be used as a base on which to build an updated set of rights primed for the digital age.

Previously the 'child' was largely a passive recipient of rights, but in the digital world children need to take a more active role, as children are full participants in the digital environment, the whole of society needs to be involved in their safe participation. Schools and parents took the lion's share of responsibility in the past because they had most control of what children's lives touched upon. Now children's lives have a wider range of touch-points, digitally enabled, beyond the confines of the home and school.

Much as the Government has said that online and offline threats are one and the same, digital and real rights need to be indivisible also. Consequently, we need to take existing rights and rigorously apply them in the online world. By doing so, we have the potential to strengthen the position of children online, while creating a defined basis of rights.

Supporting students in schools against online harms

Being able to reach out to parents who do not have a high level of awareness regarding digital technology is an important aspect when it comes to reducing risk, especially when their child may be the victim of these risks. It is a challenge for parents to stay up to date with technological change with children often being at the cutting edge of it. The policies in the strategy that will help in this respect, such as building messages into online platforms for parents, are welcomed and it is hoped that the aim of unifying much of the existing guidance under the UKCCIS, as well as findings gaps in existing knowledge, is followed up in short order.

Another way to better support students is through cultivating an increased understanding of online safety for all teachers, irrespective of whether they are teaching subjects such as computer science. Having an up-to-date understanding of what online life is like for children is only likely to become more

[5] http://www.bcs.org/upload/pdf/peel-discussion-report_1.pdf

important. This type of ongoing learning could be implemented via making it a part of continuing professional development for teachers.

Steps like this will work best if they are applied across the country as a whole. Some schools, especially Academies in and around London, have a high level of awareness on how to safeguard children from inappropriate material, but this depth of understanding is not universal.

Improved online peer support in schools

A key worry about this strategy was the fact that it relies on teachers, parents or institutions such as schools or social media companies being wholly responsible for disseminating guidance. With the propensity for young people to ignore guidance from these sources, having a robust system of peer support could offer an alternative route for information about safety online to be shared within schools. Rolling out the Cyber Ambassador scheme nationally could provide the appropriate infrastructure for successful peer support[6]. This should not prove too difficult, as much of the structure for doing so could be lifted from the successful Anti-Bullying Ambassador scheme.

The importance of apps

The importance placed on apps by the Government in the strategy was encouraging, as these play a huge part in the online world for young people and often are side-lined due to a focus on social media. The role of mobile phone companies is another area which ought to be looked at, especially with regard to how parents can limit the scope of their children to seeing harmful material.

There could be a requirement for mobile phone companies to have an optional monthly plan that was designed specifically for children. This sort of plan would allow parents to define what apps would be allowed, and empower them to prohibit ones that they deemed unsuitable. This could also make it easier to limit the number of apps that make use of personal data, as there is often the potential for it to be collected without direct consent. This approach would likely make it easier for parents to ensure that their children are not being exposed to inappropriate material on social media platforms.

There is also a welcome commitment by the Government to produce higher levels of parental guidance on how to keep children safe online. However, the focus on new parents is not enough and additional methods to spread safety guidance should be developed so that information is disseminated for all parents. Standards should be developed in greater depth once a White Paper has been produced and these could then be given to schools, in particular head-teachers, who could then pass these on to staff.

[6] https://www.hampshire-pcc.gov.uk/school-pupils-taught-slay-cyber-sea-monsters-gofish

Responding to online harms

Existing anti-harassment legislation

Avoiding a statutory route for upholding the Internet Safety Strategy in the first instance is an understandable approach. BCS is not convinced, however, that existing legislation provides an adequate basis to protect people and to allow law enforcement agencies to work. The intricacies and numerous ways in which online abuse can manifest and the rapid change which defines the online world can make this difficult. However, as the strategy itself mentions at length, developments such as the prominence of sexting can happen almost instantaneously and new legislation that specifically challenges online developments, rather than the current piecemeal abuse and harassment legislation, could be beneficial.

Location-based apps

The default position by many tech-organisations has been to shift towards asking customers to enable location sharing via preferences. There is certainly a need for there to be greater awareness of the dangers of location-sharing and location-based meet-up's as a corollary. Figures over the past few years from organisations such as a National Crime Agency show a significant increase in crime resulting from online dating and the GPS location aspects of these play a part[7].

Tackling this is not only a case of needing to increase awareness. Working with the creators of popular dating apps to make sure that people are aware of the implications of GPS tracking, as well as preventing children from accessing such apps underage in the first place, is key. BCS believes that this would be tricky to deal with due to the fact that meet-up apps such as Happn have a business model based on location-based meeting and consequently, making this more difficult would be in direct contravention of their business interests.

Despite this, a greater level of verification to prevent children being exposed to this sort of danger should be encouraged at the earliest opportunity, even if wider issues take a longer period of time to address.

[7] http://www.nationalcrimeagency.gov.uk/publications/670-emerging-new-threat-in-online-dating-initial-trends-in-internet-dating-initiated-serious-sexual-assaults/file