Stories of Cyber Security Combined Report

Professor Genevieve Liveley, University of Bristol

Table of Contents

SOCS Combined Report

Summary

This work forms part of a research collaboration between NCSC, RISCS, and partners at the University of Bristol, examining the potential for stories and storytelling to inform and support more effective communication of cyber security good practice and policy. The first phase mapped what the storyworld of this narrative ecosystem looks like – aiming to identify problem areas where narrative dynamics are weak and failing to engage key stakeholders. It adopts a systems thinking approach to the narrative analysis of a portfolio of stakeholder interviews to identify the Tellers, Audiences, Purposes, and Occasions (TAPO) that interact across NCSC's narrative ecosystem and analyses the dynamics of these varied interactions. The second phase translates a deeper narratological analysis of these findings into practical recommendations for using and integrating salient narrative strategies across the cyber security ecosystem. Combining narrative analysis of selected NCSC public communications (including Annual Reviews and NCSC blog posts) with stakeholder interviews, this report evaluates the usefulness of different character types, plot archetypes, and dominant metaphors and tropes in use across the cyber security ecosystem. It finds that:

- The historic relationship with GCHQ provides the NCSC with gravitas and authority. It gives the NCSC a charismatic 'backstory' or 'origin myth'.
- NCSC's strategic narrative and characterization is as a 'donor' or 'helper' – a classic mentoring or caring character whose prime function is to help 'heroes' defeat 'villains'.
- Campaigns and communications explicitly aiming to 'demystify' cyber security, the free provision of tools and services, and work supporting individuals to take charge of their own cyber security, all align well with this narratological 'donor' characterization.
- The NCSC's lexicon should limit combative or militaristic terms to describe its activities in protecting the UK from online 'threats' and cyber 'attacks'; its dominant register should reflect metaphors and narrative tropes emphasizing care and support.
- An effective narrative framing for cyber security is that of collective endeavour – in narrative terms, a quest: a narrative archetype emphasizing teamwork, optimism, and future possibilities.
- Narrative-based exercises and tools (such as storytelling, counterfactuals, and gaming) promote the sharing of learnings from mistakes and near-misses.
- Blog posts allow diverse voices and viewpoints from across the NCSC to be aired.
- Character-led and metonymic storytelling help to populate the cyber security ecosystem with people, places, names, and first-person experiences, to lend 'real world' verisimilitude, relevance, and immediacy to campaigns and reports.
- Effective communication requires a suitable lexicon, with coherent metaphors, tropes, and embedded stories.

Methodology

Narrative is a loose term and is used to describe a wide range of phenomena broadly related to storytelling and communications. Narratologists simply define narrative as 'somebody telling somebody else on some occasion and for some purposes that something happened'[1]. This definition places emphasis on narrative as an action of communication that seeks to accomplish some purpose and is the definition of narrative adopted in this study and report. In short, this definition focuses on the ***Tellers*** (who are they; what's their authority, their motivations, etc?); the ***Audiences*** (who are they; why do they care or need to hear this story, etc?); the ***Purposes*** (what's the intended audience response and future action, etc?); and the ***Occasions*** (what's the context; why is this story good or bad for this time and place, etc?) – ***TAPO***. These narrative elements of TAPO work together in the communication processes of all kinds of storytelling – film and TV scripts, advertising and marketing campaigns, the stories people share on social media platforms, and the stories covered by journalists in 24/7 news cycles – and this integration reminds us that a systems thinking approach is vital to any robust narrative analysis. In this study, therefore, close attention is given to the synergies through which these narrative elements interrelate and form part of a wider narrative ecosystem in the context of NCSC communications.[2]

For example, NCSC is itself a key ***Teller*** in this ecosystem: it provides advice and guidance to a variety of government bodies (such as DCMS, BEIS, GCHQ, Cabinet Office, Home Office); to Regulators (such as HSE, FCA, ORCIC, CAA, Ofcom, HMRC); to industry (including OES and CNI) and business; to citizens; and to citizen support groups (such as the Citizens' Advice Bureau and Which?). But NCSC is also an important ***Audience*** member too, taking on strategy and policy guidance from government; working in partnership with Regulators, Universities (including through ACEs-CSE and CDTs), Research Institutes (especially RISCS, RITICS, VeTSS, RISHES, and Turing) and UKRI Research Councils; as well as liaising with high-level security and cyber agencies at both national and international levels. NCSC's mission statement nicely articulates the diversity of these various interlocutors, as well as signalling the interconnectedness of the ***Purposes*** and ***Occasions*** which frame its complex narrative dynamics:

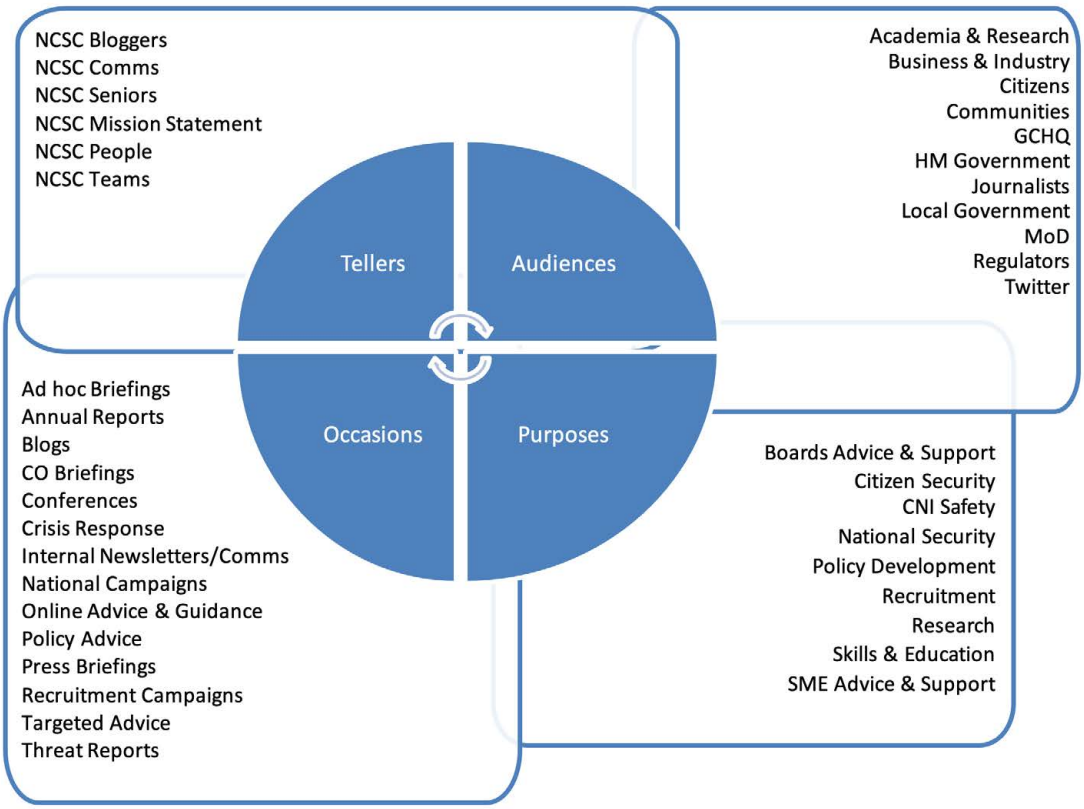
> *Helping to make the UK the safest place to live and work online. We support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.* https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

To help better understand these narrative dynamics, and to identify some of the specific TAPO interactions within the NCSC narrative ecosystem (including areas of relative strength and weakness), one-to-one semi-structured online interviews were held with 12 NCSC people and individual representatives of its key stakeholder groups in the period July to October 2021. These stakeholder insights, alongside detailed descriptions and analyses of the narrative activity associated with key TAPO components in the NCSC story ecosystem, are given in the following sections.

Ecosystem Chart

The NCSC narrative ecosystem involves a highly complex network of cyber security story narrators (or Tellers) and narratees (or Audiences), engaged in a variety of communications across a plethora of platforms (internal and external, print, digital,

social media, in-person) for a range of different Purposes, across myriad Occasions – sometimes as a matter of day-to-day routine, sometimes in response to critical incidents or threats, and sometimes in an anticipatory capacity (educating, researching, recruiting, training, advising boards, advising HMG on strategic policy, etc). In delivering its core mission, the NCSC is required to build and maintain effective communications across a particularly diverse biome: as one interviewee aptly suggested, NCSC's narrative network is like a zoo or safari park and NCSC must talk and listen to an assortment of very different animals – taking care of the safety of the general public as well as securely managing some potentially dangerous creatures (albeit, not, as yet, 'Winged Ninja Cyber Monkeys': https://www.zdnet.com/article/the-winged-ninja-cyber-monkeys-narrative-is-absolutely-wrong-former-ncsc-chief/).



Ecosystem Interactions & Issues

The stakeholder interviews unanimously approved NCSC's expertise in its metaphoric 'zoo-keeping' capabilities, warmly praising seniors for their deft communication skills, as well as commending technical, sociotechnical, research, and comms teams for their openness, friendliness, and collegiality. However, the interviews also highlighted some particular problem spaces within the NCSC's complex 'zoo-like' narrative ecosystem.

1. The History of NCSC's Relationship with GCHQ

This relationship clearly helps to provide NCSC with authority in their communications and engagements with most audiences (including HMG, Local Government, MoD, CNI, Regulators, and industry). But for some audiences (including some international collaborators, some academics, and some SMEs), this close partnership poses an ideological and/or ethical challenge and a perceived conflict of interest between the offensive and defensive divisions of national cyber security. Although NCSC is

transparent about its historic relationship to GCHQ, some interviewees questioned whether a SIGINT agency is now the most appropriate body to lead on delivering the NCSC mission.

- 'NCSC carry an amount of gravitas and if they give advice you're going to take it (because they have GCHQ behind them)'
- 'Most people don't realise the connection between NCSC and GCHQ – or that poachers and gamekeepers are living and working together'
- 'Any national security mission will be complicated by its association with an intelligence agency but NCSC has never hidden its GCHQ affiliation (a shrewd move)'
- 'GCHQ and NCSC are proud of their intelligence history/heritage … so this path dependency makes it challenging to think beyond historic trends'
- 'some are suspicious/sceptical that a government wants to 'help' corporates with security and see NCSC people as stooges'

Its relationship with GCHQ helps to provide NCSC with gravitas and influence in the configuration of its cyber security narratives, despite the potential for mistrust that the relationship might engender in some audiences. The crucial factor balancing this is the fact that NCSC is consistently transparent about its close relationship with GCHQ. Communications of all kinds celebrate this connection in all kinds of ways, consistently referring to 'the National Cyber Security Centre, a part of GCHQ'. For example, the 2019 NCSC Annual Review dedicates a full final chapter to 'Celebrating 100 years of GCHQ's cyber mission', includes a cryptogram puzzle, and explicitly flags that its CyberFirst outreach work to train the next generation of cyber security professionals includes training students and apprentices for future careers with GCHQ. The 2021 Review similarly celebrates this affiliation, including a message from Sir Jeremy Fleming, Director GCHQ – who also regularly presents at the NCSC's flagship annual conference, CyberUK.[3]

This relationship means that not everything the NCSC does or achieves can be publically narrated or celebrated, however. The CEO's Foreword to the 2019 Annual Review warns that 'we can't often talk about the operational successes and the full range of the NCSC, GCHQ and wider state capabilities' deployed in cyber security (p5). Similarly, the 2021 Annual Review acknowledges that 'As part of a national security agency not all its [the NCSC's] work can be disclosed publicly' (p3). The implications of this historic relationship and its 'untellability' for the NCSC's narrative ecosystem are nuanced.[4]

On the one hand, by openly reminding its audiences about the association with GCHQ, the NCSC reminds them of its separation from GCHQ and its distinct identity: the NCSC rhetorically distances itself from GCHQ. Indeed, as one interview emphasized: the NCSC is 'much more open, welcoming, and public-facing than its predecessors – as well as much more open to being challenged and to listening to the voices and viewpoints of a diverse range of people'.

On the other hand, the connection with GCHQ gives the NCSC a 'backstory' or 'origin myth' that enhances the authority of its current position by presenting its mission as the continuation and development of SIGINT activity and 'code-breaking' stretching back through two world wars (and explicitly evoking the secret work once carried out at Bletchley Park).[5]

In this framing, the NCSC (especially given its role as the National Technical Authority) can be seen to perform the narratological function of the 'donor' or 'helper': a mentoring or helper role which, in fairytales and traditional folktales, is often fulfilled either by a paternal figure (a wise man or wizard with arcane wisdom or magical powers of some kind – Yoda or Gandalf) or, alternatively, by a maternal figure (a supportive witch or good fairy – Cinderella's Fairy Godmother, Mary Poppins).[6] The donor or helper functions and their associated characters are typically positive forces and figures, but these functions can also promote a perception of the character or actant who fulfils it as a mystical figure, removed from the realities of everyday life; a force for good, but someone or something strange and 'other'; a magical agent with arcane knowledge who does not live in the 'real world'.

Changing the narrative in this context is a challenge. The close historic relationship with GCHQ and the respected status of the NCSC as National Technical Authority are core components of the NCSC's characterization both internally and externally. The advantages to this representation are wide-ranging: it not only assures authority and esteem, ensuring that advice and guidance issued by the NCSC is taken seriously, but (more prosaically) helps with recruitment in the highly competitive and highly paid professional field of cyber security. For, any individual working for NCSC and GCHQ is personally fulfilling the narratological function of the 'donor' through their particular contribution to and through the organisation. The mentoring or helper role at the individual level brings with it personal esteem and job satisfaction – and, in this case, the special cachet of intimate insider connections to a quasi-mystical entity.

This is not to say that NCSC individuals or teams necessarily consider themselves as belonging to a privileged tribe: to develop the Star Wars analogy suggested above, if the NCSC is Yoda then this does not entail that NCSC people therefore all identify as Jedi Knights. Indeed, as one interviewee put it: 'lots of NCSC people are really down to earth (in a Star Wars analogy, they're techies fixing droids and keeping businesses/services going)'.

However, there are disadvantages to this representation too. Those providing services and products in the wider cyber security ecosystem, those criminals operating in this space, as well as those journalists writing about threats and attackers in this domain, may be able to capitalize on the 'romance' and 'mystery' afforded by the NCSC's characterization and alignment with the narratological 'donor' function. They too can accrue esteem through the special cachet that attaches to the quasi-mystical enterprise of 'cyber security' and these actants within the ecosystem have an interest in perpetuating this narrative and its typecasting.

At the same time, such romanticizing and stereotyping of cyber security reinforces the divide between the technical experts (those initiated in its mysteries) and the non-experts (the individual citizen, sole trader, or board member, for instance, for whom cyber remains a mystery). This, in turn, can make it harder for the NCSC to persuade uninitiated non-experts to play an active part in managing their own cyber security. Campaigns and communications explicitly aiming to 'demystify' key aspects of cyber security offer a straightforward solution to this problem – and the NCSC already does this kind of storytelling and campaigning: notable work here would include the NCSC 'Exercise in a Box' and Board Toolkit.[7, 8] Importantly, these 'boxes' and 'toolkits' (available to members of the public free of charge) help to sustain and enhance the primary narrative function of the NCSC as 'donor'.

There are, then, clearly pros and cons to the fundamental characterization of the NCSC as performing the narratological function of the 'donor', the mentor or helper, the wizard with arcane wisdom or magical powers of some kind. Rather than aiming

to change this narrative configuration, therefore, it might be more desirable to understand and work with it. For example, the donor function in narrative morphologies does not work independently but always in support of a 'hero', advising and helping defeat some kind of 'villain'.[9] This perfectly describes the narrative mission of the NCSC. Maintaining – even foregrounding – this relational dynamic in its storytelling would land well with its target audiences. Indeed, this narrative configuration enables the full cast of the dramatis personae who make up NCSC's diverse audience to identify as cyber security heroes in charge of their own quest narrative, seeking to protect themselves, their employees, their businesses, their families (and the nation) from villainous criminals and threat actors.

2. The Integrated Review

The cyber security ecosystem and its narratives are further complicated by the rhetorical and strategic emphasis upon offensive cyber security in the 2021 Integrated Review of Defence, Security, Foreign and Development Policy and the subsequent launch of the National Cyber Force (NCF).[10] The offensive cyber capabilities and mission attached to the NCF are notionally very different to the more protective capabilities and mission of NCSC. Yet the NCF 'narrative' overlaps significantly with that of NCSC and interviewees questioned whether public perceptions of – as well as trust in – the NCSC could be compromised in the future as a result. Indeed, the tension in play between NCSC's current role as 'guardian' and 'advisor' and the NCF's new role as a more combative/aggressive 'force' has the potential to complicate the NCSC's future public-facing profile.

- *'We don't yet know how this will change perceptions of cyber security and the NCSC'*
- *'NCSC are national thought leaders in cyber security strategy … they're the 'guardians' of our cyber security endeavour'*
- *'The potential CoIs involved here (balancing national security with personal privacy, hard and soft securities) haven't yet hit the public discourse or consciousness (or social media)'*
- *'will the public now realise the connection between NCSC and GCHQ and trust in the NCSC be soured?'*

The NCSC's wider relationships (as part of GCHQ) with the MoD and the National Cyber Force (NCF) potentially put pressure upon NCSC's own narrative configuration and identity, therefore.[11]

The NCF is a joint military-intelligence organisation which draws together a team of different agencies with historic responsibilities and activities in offensive cyber security, and its broad mission is 'to conduct offensive operations against hostile state actors, terrorists and serious organised criminals'. [12] Its Commander is from GCHQ, although the NCF itself is not a formal part of GCHQ, as is the case with the NCSC. Clear distinctions between offensive and defensive cyber security operations are not easily drawn and the scope of the NCF remit has not been publically disclosed, meaning that public perceptions of the NCSC's own remit and 'narrative function' could become blurred.

The NCSC appears already to be anticipating and managing this risk, however. For example, the Annual Reviews employ a lexicon in which combative terms and tropes are regularly used to describe NCSC activities. The emphasis is certainly more defensive than offensive but the language register that permeates these reports is often combative. Features draw attention to the work of the NCSC in 'protecting' the UK from online 'threats' and cyber 'attacks'; 'safeguarding' citizens; advising on cyber

'defences'; working with law 'enforcement'; and 'defending' democracy. A feature in the 2020 NCSC Annual Review championing the NCSC's newly launched SERS (Suspicious Email Reporting Service) even calls for citizens to 'take up arms' and engage in 'social policing'. This quasi-militaristic and bellicose idiom is amplified by some of the key NCSC partnerships that the 2020 report highlights, including the City of London Police, the MoD, and GCHQ.

Alongside (and in contrast to) this combative language, the Annual Reviews also employ a lexicon which displays a subtle yet sustained balancing of combative terms and tropes with supportive terms and tropes. The fighting talk is combined with a parallel register of care. The NCSC 'advises', 'helps' and 'supports' others to respond appropriately to cyber security 'incidents' and 'alerts'. Indeed, alongside its accounts of the NCSC's defensive activities, the Reviews highlight the work of the NCSC in incident and risk 'management'; 'supporting' individuals, businesses, CNI, the health sector, academics, government, farmers, etc; 'encouraging' stakeholders across the cyber security ecosystem; 'deterring' hostile actors; 'identifying' threats, risks, vulnerabilities, perpetrators, and suspicious activity; 'tackling' and 'mitigating' the impacts of these. Aligned with this pattern, it is also noticeable that the NCSC's partnership with the MoD receives only a modest feature (p48) in the 2021 Review (and no explicit reference at all is made to the NCF).

In its annual Reviews, the NCSC regularly foregrounds its established characterization as a technical 'expert' providing global 'thought leadership'. This idiom is closely aligned with the narrative function in which the NCSC acts as the 'donor' character (discussed above). However, in a subtle shift away from the narrative register found in previous Reviews (and in cyber security discourse more widely), the value of the NCSC's particular technical expertise is explicitly figured in the 2021 report not (only) as providing protection or defences from cyber threats, but (also) as providing freedoms: for example, a full chapter is dedicated to celebrating the role of the NCSC in 'advancing UK leadership in support of a free, open, peaceful and secure cyberspace' (p80). Here, and in allusions across the 2021 Review, the role of the NCSC is closely aligned with the narrative 'donor' function – helping, mentoring, advising, and supporting others. This established and esteemed 'function' should help to maintain a narratological air-gap between the NCSC and the NCF in future communications and characterizations by circumscribing the NCSC's particular domain of expertise in providing support, help, advice, guidance, thought leadership, etc.

3. Clearance and Clarity in External Communications

Relating to the NCSC's important and evolving relationships with both GCHQ and MoD, external stakeholder interviews flagged security clearance issues as one of the main barriers to effective two-way communication within this narrative ecosystem. Their sense is that NCSC can (necessarily) only ever tell them part of a story. Some interviewees raised the problem of information sharing across high and low sides as one issue of potential complication, but the point was also made that information-sharing in the security profession and space more generally is not always well done.

- *'NCSC can give hints about risks/threats but not much more because of clearance issues'*
- *'Classification issues and boundaries between NCSC and outsiders will necessarily continue as pinch-points in collaborations and comms'*
- *'Because only certain grades can access certain areas, comms can become Chinese whispers'*

- *'Information sharing in security … is quite poor; people don't share best practice or errors'*

Security clearance issues are inevitably one of the barriers to effective two-way communication within the cyber security ecosystem. However, put baldly, this is what it is. There are no narrative solutions to this perceived problem. Indeed, from a narratological perspective, it is questionable whether this constitutes a genuine communication problem. As discussed above, the NCSC gains significant authority and credibility from being a part of GCHQ and from its access to sensitive or secret intelligence. Openly acknowledging the restrictions that this places upon NCSC communications is something that already happens: for example, in the 2021 Annual Review's opening caveat that 'As part of a national security agency not all its work can be disclosed publicly' (p3); and in the tag that accompanies NCSC's weekly threat reports on its website, warning that this information 'is drawn from recent open source reporting'.[13]

In fact, the NCSC appears to be highly transparent about the material it must necessarily keep secret. It makes efforts to 'tell' its audiences about those aspects of its work which are 'untellable'. The 2019 Annual Review, for example, includes a feature on NCSC's Operations Directorate, which at the time led the government response 'to counter and disrupt the UK's adversaries, capabilities and operations' – heading the article with the caveat that 'much of the team's work is secret by necessity' (p43). This Review also includes updates on the NCSC's IOC – Indicator of Compromise – machine and its role in declassifying data from the NCSC's 'top secret computers' so that it can be shared with people outside of the organization (p48).[14]

In the story world of folktales, the donor character is not usually quizzed by the hero about the source of his or her special knowledge: the hero simply takes on trust the information and advice on offer in order to act swiftly upon it. It is understandable that some stakeholders in the real world respond differently and would prefer to understand for themselves the intelligence on which NCSC advice and recommendations are made. Yet, it is unclear whether the withholding of this information impacts negatively upon communications or relations (either in the real world or the story world).

One closely related problem area does merit deeper consideration, however. Some interviewees flagged concerns that information-exchange (in the context of sharing best practice or mistakes and near-misses) across the cyber security ecosystem is relatively poor, particularly in comparison with disciplines such as aviation, safety, defence, policing, or medicine. There are good reasons why this might be the case and why sharing information, particularly relating to mistakes and near-miss experiences, might be particularly problematic.[15] There are also excellent reasons why it is good practice for the community to discuss mistakes and near-misses (a recent example being the breach of a content-management system at one of Australia's water suppliers, Sunwater, in December 2021 which had the potential to escalate into a crisis like that of Colonial Pipeline).[16] Indeed, the NCSC already includes learning from near-misses in order to better prepare for future incidents in its Board Toolkit.[17]

Narrative-based exercises have been shown to offer a useful way of addressing this issue. Storytelling and narrative-based gaming allow for anonymity to be preserved through the cloak of fictionality, while the salient lessons learned from mistakes and near-misses are drawn out and discussed. Awais Rashid and Sylvain Frey's Lego-based game 'Decisions and Disruptions' provides a series of pre-set narrative scenarios to help stakeholders explore cyber security decision-making behaviours in critical infrastructure contexts.[18],[19] Players are not explicitly directed to consider real world

near misses or mistakes (fictional or real) but the game offers the scope for teams to explore such issues (and an extension pack might help consolidate and direct this opportunity further). RISCS (in collaboration with CyRes and FLiNT) has produced a storybook of future news media stories on the theme of cyber resilience and safety inspired by real news stories and designed to help Boards identify learning points from future scenarios in order to inform actions in the present.[20] Again, Boards are not explicitly directed to consider real world near misses or mistakes but the stories offer the scope for them to explore such issues (and a second edition of such stories might further focus on this opportunity).

In this context, the use of counterfactuals can also be of particular value – enabling Boards to discuss what could have happened in their own organisations, what their responsibilities and liabilities would be if the counterfactual came to play out in actuality, and what should be done to prepare for and mitigate this possibility. Indeed, some interviewees suggested that 'near-miss' and 'counterfactual' stories offer especially useful narrative tools in cyber security as they allow the NCSC to communicate 'real world' impact in the absence of actual crisis stories.

4. The Atomisation of NCSC Tellers

The diversity and breadth of NCSC's mission requires a matching diversity and breadth in the make-up of the organisation itself. This necessarily results in a certain degree of atomisation of different units and teams, and the compartmentalisation or siloing of different internal sub-missions – along with the narratives they tell about themselves and each other. In turn, this supports a culture of implicit team tribalism and a tacit hierarchy privileging certain sub-missions and the units or teams that support them. For example, technical teams working on CNI, hostile nation state actors, or serious organised crime tend generally to be accorded greater authority in this ecosystem than sociotechnical research or comms teams. Indeed, the more specialist, high threat, and technical the sub-mission, the higher the status of the associated team and the 'characters' who deliver it – and the greater the authority afforded their role as story tellers. This culture or habitus particularly privileges the 'Uber-Techie' both as a leading narrative character and narrator. Interviewees suggested that the history of NCSC (both as National Technical Authority and as part of GCHQ) combined with the breadth of its remit contributed to the development of this 'Techie' culture.

- *'At its core, NCSC is the National Technical Authority – but it is doing (well) lots of things it wasn't originally set up to do'*
- *'There is effectively an air-gapped zone between different parts of the NCSC'*
- *'Different characters and sectors within the ecosystem speak different languages'*
- *'There's definitely a cultural hierarchy within/across NCSC that places protecting critical national infrastructure at the top and general public online safety lower down (justly so)'*
- *'fundamentally each NCSC unit and team is focused upon its own mission'*
- *'This world is ideologically charged and tribal'*
- *'There's limited awareness both internally and externally of the inter-connecting parts that NCSC (and others) play in a much bigger Cyber narrative'*
- *'There is real pride in being 'technical"*

- *'There are often 2 tribes or camps (one research-led, the other practice-led); the practical/technical tribe can object to the 'navel gazing' of the researchers, object to 'over-complicating' problems and problem-solving, and be resistant to new ways, new ideas and new thinking'*

The privileged status of the 'Uber-Techie' character in this ecosystem is one manifestation of the narratological donor function that the NCSC as an organisation fulfils (as discussed above). Reframing this privilege within the current configuration of the system would be challenging (and would potentially destabilize some of the important benefits that this existing dynamic offers).

The concerns of stakeholders in the ecosystem who experience this culture as problematic, however, could be addressed in some degree through narrative-based interventions. For example, NCSC blog posts offer the opportunity for different voices and viewpoints from across the organisation to be heard.[21] As relatively informal story texts with a fast-track to publication, blogs were described by one interviewee as a way 'to oxygenate new ideas, and establish some authority for those ideas, to start (or stop) a contentious conversation'. As a mode of storytelling which showcases a personal point of view in this conversational (or epistolary) style, blog posts credit individual 'characters' within the wider narrative ecosystem with immediate narrative authority simply through the act of first-person storytelling and thereby represent a distinctive and democratic narrative form.[22] Soliciting regular blog posts from across the NCSC ecosystem would offer a positive way to diversify the organisational culture in terms of enabling different voices and viewpoints to be communicated.

The Annual Reviews also offer an excellent narrative platform for celebrating stories about the broad range of activities carried out by different teams. For example, in the 2021 Review, Lindy Cameron personally acknowledges the great diversity and range of the different teams and individuals who each contribute to the success of the NCSC mission (p86). Indeed, the 2020 Annual Review's master trope explicitly exploits the idea of shared purpose and teamwork in its elaboration of the idea that 'cyber security is a team sport'.

The claim itself is reiterated on a number of occasions; the metaphor is illustrated with an action shot from a rugby game; dramatized through a series of case studies featuring sports-themed online scams; personified with a featured stakeholder character and former rugby player; extended to include the Five Eyes cyber security incident-response 'playbook'; and (subtly) underscored by mention of NCSC's political relationship with DCMS – the Department for Digital, Culture, Media, and Sport.[23] Although, the team sport metaphor (especially in literal mode) necessarily has its limitations, the team dynamic is a powerful narrative device that plays well across the cyber security ecosystem and merits its prominence in NCSC communications (see below on the importance of the team metaphor to the NCSC's 'quest' mission and narrative).

5. The Atomisation of NCSC Audiences

Such atomisation has further implications for the effectiveness of the different messages and narratives that NCSC needs to communicate to its different stakeholder audience groups. Interviewees highlighted as a problem the fact that different audiences may receive essentially the same 'technical' advice from NCSC, despite significant differences in their actual interests and requirements. Regulators of CNI, CEOs and CESOs of small businesses, and individual citizens each need tailor-made advice and narratives that are framed to speak directly to their individual interests if that advice is to achieve its purpose – an issue described by a number of interviewees

as 'a translation problem' (anticipating some of the problems of language and rhetoric in NCSC narratives discussed below).

- *'NCSC is used to dealing with the high threat club (nation state actors, serious organised crime) and extends the same narrative, language, tools, approaches to individuals and business'*
- *'the same tech teams provide the same advice for all types of audience – from citizens to critical infrastructure'*
- *'The Cyber Aware programme aims to tailor the framing of NCSC advice to make it more obviously relevant and salient to particular audiences (e.g., farmers, early years carers, etc) – it's essentially the same guidance but it's re-framed around the specific needs of particular groups'*

The NCSC website already does a good job of offering tailor-made advice to particular audiences within the cyber security ecosystem. Topics are explicitly tagged as 'written for' specific stakeholder groups:

- Cyber Security Professionals
- Individuals & Families
- Large Organisations
- Public Sector
- Self Employed & Sole Traders
- Small & Medium Sized Organisations

Campaigns are also targeted at individual groups and sectors with tailored advice and guidance having been developed in recent years for, e.g:

- Boards
- Charities
- Farmers
- Early Years Carers
- Schools & School/College Governors
- Online Shoppers & Retailers
- Universities & Academics
- Home Workers
- Sports

The NCSC is also improving its narrative configuration of (and communications with) the 'victims' of cyber attacks and online scams. For example, in the 2021 Review, not only was the word 'victim' itself used with less frequency (26 references compared with 39 in 2020) but the discussion of 'victims' was confined to a narrower range, with only a selection of key chapters featuring this characterization. The 'victims' of ransomware attacks and other cyber threats are aptly recognized as such in these features but they are not the focus of the narratives here. Idiomatic references to 'falling victim' to online scams, etc, appear on only two occasions, and there is no sign in the 2021 Review of the subtle 'victim blaming' seen in other parts of the cyber security narrative ecosystem (although, a hint of this rhetoric is perhaps visible in the generalized charge made (p34) that 'many organisations are still not managing their cyber risk effectively'.[24]

However, the 2021 Review as a whole marks something of a sea change in the representation of those individuals and organisations who do experience cyber crime. For example, in the 2020 Review, competing against the metaphor that figures cyber security as a team sport, the 'victims' of cyber crime are positioned as non-team-players. A 'Cyber Aware' feature engages in the discourse and rhetoric of victim blaming, characterizing 'the public' as an anonymous blocking agent. Indeed, the narrative logic of victim blaming positions the victim as a narratological 'opponent' character, actively hindering the work of the NCSC.

Elsewhere in the report we see the stereotyped 'othering' of the victim as a lazy or careless non-team-player responsible for letting the rest of the side down (p64):

> *Most of the cyber threats to the public are high-volume, low-sophistication attacks which can be prevented with just a few actions. However, a considerable proportion of the public are not taking the simple steps to protect themselves.*

Similarly, a feature on ransomware (p86) asks the audience 'how can you avoid being a victim?' – and again characterizes victim status (for both individual citizens and organisations) as unnecessary and readily preventable. The featured 'victim testimonial' (p90) is presented in the mode of a simple event-based 'story'– a basic chronolinear narrative (first A happened, then B happened, then C ...). But this was a missed opportunity within the report to represent a 'survivor' story of cyber crime in a more nuanced and dynamic style – emphasizing causality and consequentiality more (B happened because of A, which led to C). This was also a missed opportunity to tell a compelling 'good news story' showcasing NCSC's fast-acting and wide-ranging responses to the report of an attack.

Noteworthy in this context is the default tendency in natural language discourse to characterize a victim of attack or crime as a tragic type: that is, individual citizens and organisations are represented not only as victims of cyber crime but as victims of fate or chance: metaphorically, they 'fall victim to a phishing attempt' (p23); or 'fall victim to cyber crime' (p51, 57, 64). Indeed, the feature on 'Exercise in a Box' (despite its compelling use of simile – likening cyber attack exercises to fire drills) neatly illustrates this natural language combination of victimhood and bad luck or fate (p57):

> *We urge business leaders to treat Exercise in a Box in the same way they do their regular fire drills – doing so will help reduce the chances of falling victim to future cyber attacks.*

Such formulations and metaphors can be hard to avoid, but their pervasive or unguarded use can result in the unintended configuration of the victim of a cyber attack (whether an organization or a person) as simply unlucky – denying them agency and modelling their role as one of essential passivity and helplessness (as they await the aid and expertise of the NCSC team to come to the rescue). Indeed, the 2019 Review reports one finding of the UK Cyber Survey: 'that people are concerned, confused and, to some extent, fatalistic that they will become victims of cyber crime' (p14). Whereas victim blaming places undue emphasis upon the personal responsibility of individuals to keep themselves safe, the rhetorical pendulum can easily swing in the other direction and place undue emphasis upon their inability to take preventative and protective action in the face of unpredictable and capricious (unseen) forces. This can set up conflicting narrative dynamics and undermine the intended message of public-facing communications aiming to empower citizens, businesses, Boards, etc, to take charge of their own cyber security.

The narrative concept and characterization of 'victim' is already a highly complex term conferring a negative and passive status: it connotes 'prey', 'target', 'dupe', 'casualty',

'sufferer', 'wounded or injured party' – a passive object rather than an active subject, lacking independent agency.[25] In the story world it forms part of a character triad, engaged in close relationships with a story's antagonist(s) – the bad guy(s) who mean harm (here the cyber criminals) – and with the protagonist(s) – the good guy(s) whose role is to protect, defend, help (here the NCSC).

A 'victim' typically demands an audience's empathy – but this can be compromised when a narrative focuses on enumerating the number of victims (or scale of harms) rather than upon the experience of the individual. Empathy is similarly compromised by anonymity. In this light, although it is certainly sensible and useful to refer to 'victims of cyber crime' in NCSC communications, appeals to anonymous numbers of any group of victims makes these faceless characters difficult to empathize with, and their stories lose affect.

Research into the effects and affects of narrative dynamics in environmental and humanitarian disaster stories suggests that audiences find it hard to engage with accounts featuring multiple and/or anonymous 'victims'.[26] In order for such stories to be compelling, audiences prefer to follow the individual experience and story-line of a named individual who brings the story to life for them. Dillon and Craig (2021) describe this form of narration as 'metonymic' storytelling and argue that 'metonymically legitimate charismatic stories can serve an important function in drawing attention to a policy matter (a complicated or complex system of some kind) and in framing that matter in an affective way.'[27] Indeed, they caution that the power of metonymic storytelling is such that tellers should always ensure that the individual narrative they choose to highlight is 'legitimate' – that is, that it genuinely represents the wider experience of others in this context. Alongside the anonymous victim statistics reported in the NCSC's Annual Reviews (and other communications), then, a more powerful affect could be achieved by offering narrative case studies and testimonies telling the stories of real people – albeit, remaining always mindful of the importance of ensuring the metonymic legitimacy of their narratives.

This focus on individual 'characters' through character-led metonymic storytelling not only offers the opportunity to engage audience empathy and bring the experience to life for them, but reconfigures the passive 'victim' story – the tragic bad news story – into an active 'survivor' or good news story.[28] The resulting narrative dynamic emphasizes the positive actions that can be taken when people are faced with an attack. It will also foreground the relationship between victim/survivor and NCSC protagonist as a partnership in which both work together on the same team in order to tackle a challenge and combat the antagonist. As the 2020 Review puts it, foregrounding the role of the NCSC as 'working for and with the citizen' (p51). In turn, this can help to shift the underlying narrative archetype from a tragic emplotment (where chance, bad luck, and helplessness in the face of attack feature highly) to that of the quest (where teams taking on challenges together take centre stage).

6. The Politics of Cyber Security Stories

External stakeholders (i.e, non-NCSC interviewees) drew attention to the increasing politicization of cyber security and its narratives – that is, the complication of NCSC narrative purpose(s) as a result of shifts in government thinking. The Integrated Review represents one prominent problem area in this respect – particularly the ambition to use national security assets to help support the levelling-up agenda and economic recovery and growth as the UK seeks to become a 'Science Super-power', building and sustaining strategic advantage through innovations in its cyber capability. Some external stakeholders in the Regulation domain also observed that a

new political dimension had been introduced to their relationship with NCSC as a result of government reform, and that the already stretching NCSC remit was in a phase of rapid – politically driven – evolution.

- *'This Government believes that true prosperity depends on the levelling-up of opportunity and doing more to share the benefits of economic growth across the UK. It also believes that our prosperity and security are mutually reinforcing'*
- *'The narrative to emerge from the 2021 Integrated Review is that the UK is a global cyber power, aiming to reap all the benefits of a cyber future to survive and thrive – as well as supporting the levelling up agenda, net zero plans, skilled workforce, etc.'*
- *'as political colours and priorities change, so messaging can change – introducing tension between the technical and political dimensions and between advising and policing this space'*
- *'NCSC and its remit is changing and evolving rapidly'*

As part of HMG, with a critical national mission – including national security – some political colouring of NCSC's work is unavoidable. In its public-facing communications this is particularly prominent in the ministerial headline-speakers at the annual CyberUK conferences and the 'Ministerial Forewords' with which each Annual Review opens. These help to establish the overarching theme or motif for each year's narrative overview by emphasizing, for example, the real world impact of NCSC's activities (2021) or the critical role of cyber security to the UK's economic resilience and recovery post Covid (2020).

The importance of cyber security to the UK's safe governance is also further amplified in regular features within the Reviews focusing upon the NCSC's work with Devolved and Local Governments. The 2021 Annual Review repeatedly refers to aspects of the UK 'government', making clear the privileged status of HMG as both Teller and Audience in this ecosystem. Close reading, however, suggests that the 'economy' represents the most overt, persistent, and proliferating topic aligned with the politicization of cyber security.

In the 2019 Review, the connection between economic prosperity and cyber security is briefly mentioned but is not a dominant feature of the narrative: the report characterizes the mission of the NCSC as 'protecting citizens and the wider economy from harm' (p13); 'ensuring a secure, resilient and prosperous economy by providing people and organisations with the cyber security skills they need' (p68); and working with DCMS to support economic sectors. It also flags the potential damage to the economy threatened by cyber attacks against CNI (p31).

In the 2021 Review, the connection between the economy and cyber security recurs on 9 occasions – typically in the context of NCSC's support for key contributors to the UK economy such as the Space sector and Sport. Other NCSC activities are similarly positioned in economic contexts, including work towards protecting supply chains; 'piloting products and tools to defend critical areas of the UK's economy and society' (p72); and 'helping to open up opportunities to sell UK cyber security products and services to foreign markets' (p77).

This emphasis upon the imbrication between the UK's economy and cyber security aligns with the overarching narrative of the 2021 Integrated Review which explicitly proposes the use of national security assets to support the government's levelling up agenda: 'This Government believes that true prosperity depends on the levelling-up of opportunity and doing more to share the benefits of economic growth across the UK. It also believes that our prosperity and security are mutually reinforcing.'[29] This

government ambition creates an alternative narrative and mission for the NCSC that puts economic growth, levelling up, and jobs creation on a par with making the UK a safe place to live and work online. As one interviewee put it, there is 'a key sub-plot to the NCSC narrative – that the goal is not just to stop bad stuff happening but to make people feel safe (and thereby speed up adoption and bolster the economy)'. Indeed, the interview suggested that even before the publication of the Integrated Review, this economic 'sub-plot' was already part of the NCSC's story and was fostered by the annual NCSC Mandatory Legalities Programme for all NCSC employees – 'which sets out personal and collective responsibilities for supporting and promoting national security and the economy, and fighting serious organised crime'.

In this light, there is a potential conflict between the narrative dynamics encoded in NCSC's key mission statement and those encoded in government communications concerning its current and future role(s). The NCSC's mission statement is a narrative device which frames the work of the NCSC as part of a collective 'quest' in which each and every part of the organization has a crucial part to play – whether supporting CNI, national security, or citizens; whether engaged in public education campaigns or sociotechnical research (on the value of this collective quest to the cohesion of the NCSC's often atomized teams, see above). That quest involves: [30]

> *Helping to make the UK the safest place to live and work online. We support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.*

The mission statement represents a clear strategic narrative in that it represents the NCSC as a characterful agent, describes its purpose and goal, and outlines (emplots) the actions necessary to realize that goal. Similar organisational strategic narratives are widely adopted as framing devices by businesses, regulatory agencies, and military organizations (including IBM and Starbucks, NATO and OFGEM). Like the strategic narratives adopted by those organisations, the NCSC strategic narrative:

- has a clear purpose or telos
- evokes affect and sentiment
- aims to engage a broad range of stakeholders, internal and external
- creates the voice and vision of a reliable narrator

A strategic narrative is the story through which an organization like NCSC defines its character. This includes the use of a memorable summary or tagline – 'Helping to make the UK the safest place to live and work online'. To date, the NCSC's core mission (and strategic narrative) has been neatly aligned with its core narratological function of the 'donor' – the mentor or helper character (see above). This function and characterization is certainly not incompatible with a public role fostering economic prosperity, but there is a risk that this secondary political mission could come to blur the focus of the NCSC's primary mission.

Strategic narratives have been described as organisational micro-narratives which create 'a context of human connection, collaborating around a shared purpose, and connecting with the company's DNA'. [31] The sense of 'shared purpose' is a vital element in the NCSC's mission and the strategic narrative this emplots. It also finds purchase in the extensive appeals to 'teamwork' and 'partnerships' that are found across this narrative ecosystem.

In fact, several elements of the Annual Reviews position NCSC's overall mission and its team activities as part of a narrative 'quest'. Here we see the NCSC as a collective performing the narrative function and role of the donor/helper (a core element of the archetypal quest story) engaging variously in: tackling 'challenge(s)'; 'team' working; 'partnerships' (international and domestic); 'collaborations'; and dynamic working 'relationships' (particularly with Law Enforcement and the Armed Forces, including the MoD).

The quest is an enduring archetypal plot (a type found in the Odyssey, Jason and the Argonauts, Wizard of Oz, Indiana Jones, Avengers, etc – and in any crime novel, adventure or heist movie).[32] Archetypal plots and narratives are stories that follow familiar and traditional patterns, typically involving the core cast of stereotypical characters and functions first categorized by Propp.[33] These plot archetypes are found in every age and culture, organizing and communicating both individual and social sense-making. They are understood to function as an evolutionary cognitive resource to help make sense of the unknown and to connect communities. As such, they often shape not only film and TV scripts of all genres, but media and news reports, and the stories people share on social media. They are also widely used in marketing and advertising and in the strategic narratives deployed to represent businesses.[34] Indeed, 'script', 'schema', and 'frame' theories in cognitive psychology and narratology (informed by the latest insights into AI and machine learning), suggest that certain narrative archetypes and story plot patterns may be 'hard-wired' into human cognition as a mode of sense-making.[35]

The quest narrative involves a fundamentally optimistic, future-focused, and heroic plot centring around strong and collaborative leadership, individual and collective heroism, teamwork, and innovation – although quests can also involve leadership contests, and internal rivalries.[36] Quests are always goal-oriented and, although ultimate rewards – and plot pathways – can turn out to be multiple (Jason and the Argonauts ultimately get both the golden fleece and the girl), a successful quest plot is usually focused around a single goal or telos.

A political narrative combining two goals for the NCSC's quest – economic prosperity and security – potentially compromises this focused telos. Indeed, we see the complication of the archetypal quest narrative already playing out in the 2020 Annual Review. Here, the quest motif is embedded throughout the report's overarching narrative, with repeated references to teams, partnerships, collaborations, tackling challenges together, etc. However, this Review also engages with a secondary plot celebrating the role of the NCSC in supporting national economic recovery and rebirth – an apt story archetype that corresponds with the 'Covid 19 response' theme chosen as the unifying thread or emplotment for this year's report.

The narrative archetype of 'rebirth' (also known as the 'transformation' archetype) typically includes metaphors and language associated with the human body, health, medicine, etc. The 2020 Review features multiple accounts of the NCSC's support for the NHS and healthcare sector during the pandemic, and to cyber aspects of health and safety. For example, the Foreword refers to 'digital lifelines', a feature on Brexit refers to 'cyber security health checks', and references to 'transformation', 'resilience', and 'strength' recur throughout. However, the dominant metaphor is that of 'growth' – particularly in respect of economic growth – and the Review focuses on young people as key characters and agents of change in the cyber security ecosystem (from school children, apprentices, to graduates) and upon new business start-ups (such as those supported by the Cyber Accelerator).

The 2020 Review illustrates that it is possible to combine archetypal narratives successfully when there is a clear distinction between primary and secondary plot pathways and a clear understanding that one overarching narrative represents the main goal or telos and the secondary narrative represents a parallel mission or sub-plot (in much the same way that an adventure movie can incorporate a love story). In its current configuration, the NCSC's primary goal (as set out in its mission statement or strategic narrative) may have multiple dimensions but it has security as its focused telos. It is certainly possible to align this with parallel missions or sub-plots to help secure government ambitions for economic recovery, prosperity, levelling up, and even for the transformation of the UK into a 'Global Science Superpower'. However, these missions should be clearly identifiable to audiences as secondary plot pathways if they are not to undermine the coherence of the NCSC's currently strong strategic narrative.

Indeed, the same narratological principle might be seen to apply to the NCSC's future (narrative) relationship with the National Cyber Force (NCF). For the NCF, the dominant narrative archetype that structures their offensive mission within the cyber security narrative ecosystem is the traditional 'overcoming the monster' plot. This archetype is often associated with the quest type and works well as a localized subplot (especially where the antagonist is a clearly defined actant or character). For example, the NCSC already appeals to the generic tropes of overcoming the monster in some of its communications: the 2021 Annual Review includes a chapter focusing upon 'The Threat' which explicitly identifies China and Russia as the state actors (the figurative monsters) behind the most sophisticated attacks in 2020-21 and points to Iran and North Korea as emerging threats/monsters in this space. As the mission of the NCF develops, it should be unproblematic (in narrative terms) for the NCSC to continue incorporating this kind of sub-plot within its storyworld – providing its strategic narrative and the telos of its primary quest remain clearly defined to its diverse audiences.

7. Ideal World vs Real World

Several stakeholders (both external and internal to the NCSC) spoke of a breach between the 'cyber' world of NCSC and the 'real' or physical day-to-day world of business, industry, policy, and citizens – referring to a perceived communications gap between those 'tellers' advising on the principles of good cyber security and those 'audiences' expected to put such advice into practice. This disconnect was reported as a factor affecting various facets of NCSC's diverse portfolio, including: (i) regulators – whose priorities are seen as predominantly physical ('real world') safety rather than (cyber) security, and for whom (reportedly) NCSC's approach to risk reporting can sometimes seem unhelpfully opaque; (ii) industry and business leaders – whose priorities are innovation, expansion, resilience, etc, and for whom NCSC's advice on security can sometimes fail to align with day-to-day business and wider ambitions (i.e., as one interviewee put it, a 'tension exists between risk taking/innovation and security/guardianship'); and (iii) third-sector agencies and citizens – for whom, NCSC narratives, campaigns, and messaging was sometimes perceived to lack 'real world' personal relevance or local immediacy.

- *'Cyber is only part of the story'*
- *'We have to translate the potential risks and threats that NCSC identify into actual real world harms'*
- *'communicating risk across the interface between the cyber world and the real world is problematic'*

- *'The ideal point of engagement is in the real world, with concerns that are close to home and threats that are immediate/proximate – people don't care too much about abstract and distant threats'*
- *'NCSC are really skilled at problem solving and fire-fighting when external organisations are under pressure [...] NCSC are less strong at business as usual – at understanding real world concerns/cares and day-to-day issues'*
- *'Measuring real world impact of campaigns like Cyber Aware is really hard to do'*
- *'stories need to be real, close to home, about people like us, to be compelling'*

As its tools, kits, guidance, scenarios, and communications frequently emphasize, the NCSC is clearly committed to ensuring that its technical advice is not only realistic but that it has real world impact. Indeed, the overarching theme or motif for the 2021 Annual Review was precisely the 'real world impact' of NCSC's activities in the review period. As the Review succinctly highlights, although the world of cyber security can seem intangible and remote, removed from the everyday lives of most people, the real world consequences of cyber crime and its impacts upon the lives of real people are dramatic (p18):

> *While the threats came from a range of actors using an array of methods, they had one thing in common; they led to real-world impact. Life savings were stolen, critical and sensitive data was compromised, healthcare and public services were disrupted, and food and energy supplies were affected.*

By naming some of the companies and organisations directly affected by cyber attacks in the review period – as well as naming the threats and the threat actors behind them – the Review further brings to life these experiences, the lessons learned, and the future risks that similar threats pose to others. This year's report was far richer than its predecessors in terms of giving such details. In particular, one chapter describes the supply chain attacks that led to the compromise of the software company SolarWinds (which also affected the UK cloud and email security firm Mimecast) and Microsoft Exchange Servers. It further reports on ransomware attacks on Colonial Pipeline in the US (which affected fuel supplies to the East Coast); the American software firm Kaseya; the Health Service Executive in Ireland; Hackney Borough Council; and the UK university sector – including the Oxford department leading on Covid vaccine research and development.[37]

Naming such targets – and outlining the damage incurred – does much more than add colour and detail to the reportage of these ransomware stories. It effectively populates this part of the cyber security ecosystem with named 'characters' and increases the dynamism and affectivity of the reports through a mode of 'character-led storytelling'. It helps to lend 'real world' verisimilitude to the narrative, bringing relevance and immediacy to the story. It also appeals to the power of metonymic storytelling – whereby an individual company, service, or council comes to represent (to stand in for) others like it.

Indeed, the importance of bringing NCSC's narratives to life for its audiences is showcased in exemplary style in the Review's feature on 'Connected Places' (p61):

> *To help bring the risks to life in a relevant way for the public, the NCSC's Technical Director Dr Ian Levy cited the 1960's film classic, The Italian Job, which featured one of the first Hollywood depictions of a cyber attack. For the launch Dr Levy said: 'It was an attack against a city's centralised traffic management system. As part of an elaborate heist, a dodgy computer professor [played by Benny Hill] switches magnetic storage tapes for the Turin traffic control*

system to create a gridlock. Chaos ensues and the thieves escape with the gold. A similar 'gridlock' attack on a 21st-century city would have catastrophic impacts on the people who live and work there, and criminals wouldn't need physical access to the traffic control system to do it.'

As this example illustrates, storytelling (particularly character-based and metonymic storytelling) offers a powerful vehicle not only for communication but for sense-making within the cyber security ecosystem. Paradoxically, here a fictional story is employed to make a real cyber risk tangible and concrete. It uses story to make an indefinite future possibility visible – to imagine and so bring to life the cyber vulnerabilities of a future smart city. This is itself smart storytelling in action.

Part of this powerful storytelling dynamic is brought about by the authority of the Teller: here, the potency of the narrative is lent additional rhetorical influence by its connection to the voice of NCSC's Technical Director, Ian Levy. The 2021 Review also affectively draws upon the authority and the personal voice of Lindy Cameron, CEO of the NCSC, as the primary narrator of this communication. Indeed, the framing of the report with both a Foreword and final sign-off or sphragis by Lindy Cameron (p85-86) – who is even pictured at a microphone addressing a conference audience – gives the impression that the Review as a whole has been, in some way, narrated by her.

This evocation of an identifiable teller for the narrative and a personal voice for its chronicle of the year's activities is a highly affective storytelling device. The use of the first person ('I', 'me', 'my'; 'we', 'us', 'our') and direct address to the audience ('you') creates a storytelling dynamic that rhetorically connects the NCSC leader both with her wider team and with the Review's readers – creating a subtle sense of shared understanding, mutual purpose, and community. Again, this is smart storytelling in action.

8. Language, Metaphors, and Stories

The perceived disconnect between the ideals of the 'cyber security world' and the pragmatics of the 'everyday real world' (for various stakeholder groups) was repeatedly set within a wider context of challenging communication issues and a culture or habitus within NCSC (and the cyber security domain more widely) dominated by problematic metaphors, framing, and figures of speech. For example, several interviewees spoke of having to act as 'translators' helping to convey complex technical advice to non-technical audiences or translating threat reports and security advice into 'real world' language. A wider issue problematizing this part of the narrative ecosystem relates to the challenge of crafting and communicating cyber risk and security advice to audiences with messages that convey appropriate nuance and sensitivity. As one interviewee put it, 'it's hard to illustrate or narrate a compelling overarching narrative when NCSC doing its job well equates to no dramatic cyber stories or negative consequences to relate'. A lack of real world impact from cyber attack is, paradoxically, the best evidence we can hope to have of the successful real world impact of NCSC's activities. Indeed, some interviewees suggested that 'near-miss' and 'counterfactual' stories offer useful narrative tools in this context as they allow the NCSC to communicate such 'real world' impact in the absence of actual crisis stories – an important consideration given that so much of the NCSC's activities and successes happen, as one interviewee put it, 'under the radar'.

- *'the key mission is about avoiding bad things and maintaining the status quo – but that's not a compelling or dramatic narrative'*
- *'Teams are primarily concerned with prevention rather than 'slaying the monster"*

- *'bad news stories are powerful'*
- *'silence rather than stories is meaningful in this space'*

Significantly, stakeholders praised NCSC for its avoidance of the 'scare stories' and 'disaster movie tropes and plotlines' popular with professional cyber security speakers on the conference circuit, with some CESOs, and – of course – with journalists. In contrast, despite the reported fondness for 'sci-fi tropes' in NCSC and GCHQ, NCSC's own preferred framing for its communications aligns closely with public health narratives.

- *'Public health narratives dominate security world stories'*
- *'Cyber security is a hygiene/housekeeping/health issue ('Eat your greens'!)'*
- *'health and exercise metaphors prevail here'*
- *'5 cyber aware behaviours = 5 fruit and veg a day'*

However, despite NCSC's efforts to avoid dramatic or emotive narrative tropes and alarmist plotlines in its communications (characterized by one stakeholder as a 'register of fear'), some of its terminology retains a quasi-militaristic character which some stakeholders flagged as a problem area. A cultural discourse that frames cyber security in terms of "humans' (= ordinary citizens) vs security experts' or 'Us vs Users' – which one interviewee described as 'the language of drug dealing' – risks the stereotyping of good/bad guys in its narratives, and the 'othering' or alienation of key stakeholder audiences that it aims (and needs) to reach in its mission. A particular pinch point in this context is the word 'cyber' itself which carries a semantic and narrative register that some audiences find mysterious and attractive, but others find alienating.[38]

- *'The language, tools and approaches that NCSC uses routinely are storied: they seek to find 'threat actors', sources/origins, 'insider' or 'accidental' threat actors, using 'attack trees"*
- *'We still don't have the lexicon to embed and normalize cyber security and innovation into natural discourse'*
- *'This language/approach is problematic when it comes to helping non-security experts (citizens, SMEs, etc) to think seriously about cyber security'*
- *'Other narrative framings are available: security as care … a gendered narrative in which security is an unseen, undervalued work – like housework/child care'*

While certain narrative framings, discursive registers, character stereotyping, and types of figurative language were highlighted as problematic, several interviewees commended the part that NCSC seniors played on the national and international stage in communicating and translating technical material for non-technical audiences (such as the recent debunking of the 'Winged Ninja Cyber Monkeys Narrative': https://www.zdnet.com/article/the-winged-ninja-cyber-monkeys-narrative-is-absolutely-wrong-former-ncsc-chief/). There was widespread recognition among stakeholders that persuasive storytelling by authoritative experts – both in person-to-person contexts and at scale – is a highly effective form of communication for NCSC. Some interviewees also suggested that such storytelling not only helps with sense-making in this complex sociotechnical space, but also helps to manifest the immediacy (and personal relevance) of cyber risk. For example, stories concerning cyber attacks as experienced by recognizable characters, people living in the same region or working in the same profession as the target audience – 'people like us' – were recommended as more likely than global news stories featuring international state

actors or big companies to have impact on citizens and SMEs. Big news stories (such as those involving Maersk, The Big Hack, Huawei, Wannacry, Snowden, Sony, Solar Winds, and Colonial Pipeline) were characterized as 'canonical', serving as exemplary or cautionary tales for industry and business audiences.

- *'Cyber security is a highly technical topic so stories help with sense-making and provide a kind of narrative short-hand'*
- *'stories … make cyber threats more tangible, bring them closer to home, make the threat real'*
- *'The numbers involved in cyber-crime are massive so it can be easy to lose sight of the individual human stories buried below the big headlines'*
- *'soft channels for communication; person-to-person comms are crucial'*
- *'stories need to be real, close to home, about people like us, to be compelling'*
- *'there hasn't (yet) been a UK category 1 incident so it's helpful to have these stories to explain why we need to worry about cyber security – we need some stories to inform and prompt action; counterfactuals are also helpful for this; as are collections of lower scale/everyday citizen stories that don't make the headlines'*

The use of an appropriate lexicon, and the integration of suitable metaphors and embedded stories, is fundamental to the effectiveness of cyber security narratives – not least of all because the word 'cyber' itself is a problematic term which some audiences find mysterious and attractive, but others find alienating. Indeed, as one interviewee asked: 'how do you fight or protect against an abstract noun … the word 'cyber' is itself unhelpful – we need a different/better word'.

The NCSC has already demonstrated a concerted commitment to using language and metaphors sensitively.[39] However, one of its favoured tropes appears to be losing its previous appeal: the metaphor of cyber security as 'healthcare' (specifically 'hygiene'). The (pre-pandemic) 2019 Review featured the NCSC's support for the NHS and healthcare sector in the wake of the WannaCry ransomware attack of 2017 and adopts an apt healthcare metaphor to represent its own work supporting this sector as a 'Cyber health check for the NHS' (p25). The cyber security as health trope is alluded to in a quotation linking 'cyber defences and cyber hygiene' (p30); in advice for schools and colleges on good 'cyber hygiene' (p61); and in a Cyber Accelerator case study helping customers improve their 'cyber hygiene' (p80). The 2020 Review refers only briefly to 'cyber security health checks' (p38); and health-related metaphors and tropes were again largely absent from the 2021 Review, which offered only one allusion to 'cyber hygiene' – as a priority for home working during the pandemic (p55).[40]

One of the reasons that the healthcare metaphor is seemingly declining in this ecosystem is that it lacks drama and dynamism: cyber security as good hygiene aligns the cyber professional (and the NCSC) with the dentist; it posits cyber aware behaviours as the equivalent of dental flossing (or eating 5 portions of fruit and veg a day). This register is starkly at odds with the heroic quest narrative and the donor/helper function with which cyber security can confidently identify – and, as such, fails to cohere with the NCSC's core mission, public characterization, and strategic narrative. Indeed, it might be time to retire the hygiene and health metaphors from cyber security discourse altogether.

This does not mean that the broader lexicon of care also needs to be jettisoned. It is worth recalling that the narratological function of the 'donor' or 'helper' is fulfilled in the traditional or mythic storyworld not only by a wise man or wizard but also by a supportive witch or good fairy – such as Cinderella's Fairy Godmother or Mary

Poppins. In such stories, the help and support given by the donor to the hero on his or her quest is often configured explicitly as a form of affectionate care (not only for lone heroes but for children and families).[41] The metaphor of cyber security as care, therefore, fits well with the NCSC's existing core mission and strategic narrative – as well as with its widespread activities training the next generation of cyber security professionals and preparing the next generation of digital natives to safely live and work (and shop and bank) online.

One of the potential advantages of this slight shift in narrative and lexical register is that it actively reinforces the team quest narrative archetype that the NCSC has already established as part of its own strategic narrative and mission. It moves the discourse away from a simplistic protagonist vs antagonist dynamic (or 'overcoming the monster' plot) troping the NCSC (and wider cyber security services) as the 'heroes' and the cyber threat actors (from lone hackers in hoodies, to serious organized crime gangs, to hostile states) as the 'villains' – and everybody else as the hapless 'victims' passively and pessimistically awaiting the next inevitable attack.

Indeed, the power of the quest narrative is that it offers a more optimistic reconfiguration of these pessimistic cyber security characters and tropes. The quest narrative does away with the singular hero (as a potential single point of failure), and instead brings together a diverse team of different characters with specialist skills who each have a valued contribution to make to the overall success of the mission. The quest narrative also does away with the singular monster or villain. The quest is iterative, future facing, a journey rather than a battle. Its primary goal is not only the defeat or destruction of bad thing(s) but also the search for good thing(s). The quest looks to the horizon for future possibilities and profits that can be sought out and brought back home for the benefit of society as a whole.

Conclusions

Among the project's key discoveries is that the NCSC's narrative function and characterization is widely understood as that of a 'donor' or 'helper' – a classic mentoring or caring character whose prime function is often to help 'heroes' defeat 'villains'. The free provision of tools and services, and work supporting people to take charge of their own cyber security, align well with this narratological 'donor' or 'helper' characterization – as do metaphors and narrative tropes emphasizing the role of the NCSC in mentoring, advising, and supporting others.

The project has also found that one of the most effective narrative framings for cyber security is that of collective endeavour – in narrative terms, a quest: a narrative archetype emphasizing teamwork, optimism, and future possibilities. Aligned with these core narratological functions it finds that:

- The historic relationship with GCHQ provides the NCSC with gravitas and authority. It gives the NCSC a charismatic 'backstory' or 'origin myth'.
- Campaigns and communications explicitly aiming to 'demystify' cyber security, the free provision of tools and services, and work supporting individuals to take charge of their own cyber security, all align well with this narratological 'donor' characterization.
- The NCSC's lexicon should limit combative or militaristic terms to describe its activities in protecting the UK from online 'threats' and cyber 'attacks'; its dominant register should reflect metaphors and narrative tropes emphasizing care and support.
- An effective narrative framing for cyber security is that of collective endeavour emphasizing teamwork and collaboration.
- Narrative-based exercises and tools (such as storytelling, counterfactuals, and gaming) promote the sharing of learnings from mistakes and near-misses.
- Blog posts allow diverse voices and viewpoints from across the NCSC to be aired.
- Character-led and metonymic storytelling help to populate the cyber security ecosystem with people, places, names, and first-person experiences, to lend 'real world' verisimilitude, relevance, and immediacy to campaigns and reports.
- Effective communication requires a suitable lexicon, with coherent metaphors, tropes, and embedded stories.

Glossary of Narratological Terms

Actant: the structural role performed by an individual character within the narrative; including key roles and functions (sometimes paired) such as hero, opponent/villain, donor/helper, etc.

Archetype: archetypal plots and narratives are stories that follow familiar and traditional patterns, typically involving a core cast of stereotypical characters and functions; examples include the quest, 'overcoming the monster', rebirth or transformation, rags to riches, voyage and return, comedy, and tragedy.

Audience: the real or imagined addressees (or narratees) to whom a narrative communication is directed.

Backstory: the origin, prequel or background story that is understood to precede the emplotted events in the narrative; action that is chronologically earlier than the primary narrative, used to add texture, depth, and believability.

Counterfactual: a 'what if' story presenting the imagination of alternative possibilities for past or future events: what might happen, what could have happened if...?; used to explore multi-order consequences (past or future).

Emplotment: the dynamic linking together of actions and events so as to produce a plot; n.b. actions and events linked together in chronolinear sequence may produce a simple story ('The king died and then the queen died') but a plot requires the linkage to be causal ('The queen died because the king died').

First-person storytelling: the use of the first person ('I', 'me', 'my'; 'we', 'us', 'our') and direct address to the audience ('you') to create a sense of shared understanding, mutual purpose, and community.

Function: narratologists connect stereotypical characters or dramatis personae to a suite of narrative functions: villain, donor, helper, princess (or sought-for-object), dispatcher, hero, and false hero

Metonymic storytelling: the story of an individual named character or actant used to represent (to stand in for) and garner audience empathy for the experiences of multiple unnamed others.

Micro-narratives (or nano-stories): the evocation of a story world using just a few words (e.g., 'For Sale. Baby Shoes. Never Worn')

Narration: storytelling or the dynamic processes by which a narrative is communicated; for some narratologists, this represents a separate level distinct from story or plot.

Narrativity: the (contested) properties that lend a story its 'storiness'.

Narrator: the agent whose voice communicates a narrative

Narratee: the real or imagined addressees, the ideal audience to whom a narrative communication is directed (as distinct from the real or implied audience).

Plot: the dynamic arrangement and synthesis of actions and events into a coherent and affective narrative.

Sphragis: a device through which a narrator or teller identifies themselves to the audience (literally a 'seal' or 'signet')

Story world: the mimetic world conjured by the story.

Strategic narrative: a mission statement or micro-narrative which represents an organisation as a characterful agent or actant, describes its purpose and goal, and outlines (emplots) the actions necessary to realize that goal.

Tellability (and untellability): the features of a story that it make it worth telling and possible to tell (the features and contexts that make it difficult or impossible to tell a particular story).

Telos: an end, purpose, or goal, used to structure a plot and determine character/actant objective(s).

Endnotes

1 Phelan, J. (2017). *Somebody Telling Somebody Else: A Rhetorical Poetics of Narrative.* Columbus: Ohio State University Press.

2 See also Hyyryläinen, I. (2020). *Constructing the Narrative of Cyber Security as a National Security Issue : A narrative analysis on Finland's approach to cyber security (Dissertation).* Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-9351

3 For example: https://www.gchq.gov.uk/news/director-gchq-speaks-at-cyberuk-2021

4 On untellability as a narratological category see especially Baroni (2014): https://www.lhn.uni-hamburg.de/node/30.html

5 https://www.ncsc.gov.uk/information/our-history

6 Propp famously defines seven dramatis personae attached to a suite of 31 narrative functions: villain, donor, helper, princess (or sought-for-object), dispatcher, hero, and false hero (Propp, V. [1958] 2015. *Morphology of the Folktale*, edited with an introduction by Svatava Pirkova-Jakobson, translated by Laurence Scott). Lévi-Strauss (1955) would later reconceive Propp's narrative functions into narrative events (Levi-Strauss, C. 1955. 'The Structural Study of Myth', *The Journal of American Folklore*, 68:270: 428-444); Greimas (1966) (Greimas, A.J. [1966] 1983. *Structural Semantics: An Attempt at a Method*, Lincoln and London: University of Nebraska Press) and Bremond (1980) (Bremond, C. 1980. '*The Logic of Narrative Possibilities*', New Literary History, 11:3: 387-411) would go on to reformulate Propp's functions into their own narrative grammars, comprising paired character or actantial functions including: the hero/subject and his search for an object/person; the hero's helper/donor and the villain/ false hero/opponent. In fact, Propp (1958: 35) already fuses the functions and characters of donor and helper: 'the hero is tested, interrogated, attacked, etc. , which prepares the way for his receiving either a magical agent or helper (first function of the donor)'. See also Jameson, F. (2013). The Political Unconscious: the function of the donor finds manifestation in two distinct groups of characters, the supportive or maternal women figures and the spiritual fathers' (112). Kafalenos, E. (1997). '*Functions after Propp: Words to Talk about How we Read Narrative*', Poetics Today, 18:4: 469-494, maps the limitations of Propp's Morphology but acknowledges that Propp nevertheless 'offers a vocabulary to talk about how we read narratives' (470).

7 https://www.ncsc.gov.uk/information/exercise-in-a-box

8 https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

9 A common logic in Propp (1958), Lévi-Strauss (1955), Greimas (1966), and Bremond (1980).

10 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

11 The publication of the 2022 National Cyber Strategy clarifies some of these issues and confirms that the ambition for the latest strategy is to see the NCSC and NCF (together with GCHQ and MoD) working closely together: https://www.gov.uk/government/publications/national-cyber-strategy-2022

12 https://www.kcl.ac.uk/policy-institute/research-analysis/national-cyber-force

13 For example: https://www.ncsc.gov.uk/report/weekly-threat-report-3rd-december-2021

14 There is a marked decrease in the references to 'secret' materials and activities in the 2020 and 2021 Reviews, however. In the 2021 report, the only such reference is to 'UK's commercial secrets' (p190).

15 See the 2018 University of Colorado study by Bair, Bellovin, Manley, Reid, and Shostack: https://ctlj.colorado.edu/wp-content/uploads/2018/09/4-Shostack-8.7.18-FINAL.pdf

16 https://securitybrief.asia/story/the-problem-with-near-misses-in-cybersecurity

17 https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

18 http://scc-research.lancs.ac.uk/sites/decisions-disruptions.org/assets/dd_rules_final_nb.pdf

19 https://crestresearch.ac.uk/comment/cyber-security-decisions/

20 https://www.riscs.org.uk/anticipation-prospection/

21 https://www.ncsc.gov.uk/section/keep-up-to-date/all-blogs?q=&defaultTypes=blog-post&sort=date%2Bdesc

22 https://www.researchgate.net/publication/228176224_Blogs_and_the_Narrativity_of_Experience

23 Similarly, although the 2020 Review's master trope that 'cyber security is a team sport' is absent from the 2021 report, the metaphor of the 'team' endures throughout.

24 This change in the characterization of 'victims' of cyber attacks aligns well with the 2021 Review's emphasis upon 'resilience'. See also, Emma W's 2017 blog post correcting the false narrative that 'people are the weakest link in security': https://www.ncsc.gov.uk/blog-post/cyberuk-unsung-heroes-cyber-security

25 See OED s.v.

26 On this phenomenon in the reporting of environmental harms and victims see especially Heise, *U. K. Sense of Place and Sense of Planet: The Environmental Imagination of the Global*. Oxford: Oxford University Press, 2008. See also Dillon, S. and Craig, C., 2021. *Storylistening: Narrative evidence and public reasoning*. Routledge.

27 Dillon, S. and Craig, C., 2021. *Storylistening: Narrative evidence and public reasoning.* Routledge.

28 On characterful and character-led storytelling see Liveley, G., Slocombe, W. and Spiers, E., 2021. Futures literacy through narrative. *Futures, 125*: https://www.sciencedirect.com/science/article/abs/pii/S0016328720301531?via%3Dihub

29 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

30 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

31 https://hbr.org/2016/03/how-to-build-a-strategic-narrative

32 Booker's popular thesis (heavily indebted to both Propp and Aristotle) claims that there are seven basic plot archetypes: (Booker 2004), such as 'Overcoming the Monster', 'Quest', 'Transformation', or 'Voyage and Return'.

33 Propp, V. [1958] 2015. *Morphology of the Folktale*, edited with an introduction by Svatava Pirkova-Jakobson, translated by Laurence Scott

34 https://www.researchgate.net/publication/333968807_The_sympathetic_plot_Identifying_and_explaining_a_narrative_universal/link/5d0fe43892851cf440463df1/download

35 Research into archetypal and generic narratives in scientific and environment/climate understanding has been conducted by the Royal Society (https://royalsociety.org/-/media/policy/projects/ai-narratives/AI-narratives-workshop-findings.pdf) and British Academy/ESCR (https://www.narrative-science.org/events-narrative-science-project-workshops-environment.html).

36 On archetypes and narrative see: https://doi.org/10.1080/1047840X.2019.1614808. The quest plot is an exceptionally flexible narrative form which can also embrace multiple internal sub-plots: that is, it can coherently integrate parallel or tangent storylines that predominantly appeal to other archetypal plots, such as 'tragedy', 'transformation and rebirth' or 'overcoming the monster'.

37 Appealing to a canonical or exemplary cyber security story from previous years, the Review reports that the success of the NCSC engagements with universities such as Oxford during the pandemic drew upon experiences and learning from the WannaCry ransomware attack in 2017.

38 See also Busse, K., Seifert, J., and Smith, M. (2020). Exploring the security narrative in the work context, ***Journal of Cybersecurity***, Volume 6, Issue 1, 2020: https://doi.org/10.1093/cybsec/tyaa011

39 See also Emma W's 2020 blog post calling for an overdue change in cyber terminology: https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white

40 References to cyber security as cyber hygiene and health also appear to be in decline on the NCSC website. For a recent (July 2021) exception see: https://www.ncsc.gov.uk/collection/zero-trust-architecture/assess-user-behaviour-service-and-device-health

41 On cyber security as a form of care see especially: Hamilton, J. T. (2016). *Security: Politics, humanity, and the philology of care*. Princeton University Press; and Starr, S.L. (1999). *The Ecology of Visible and Invisible Work*: https://link.springer.com/article/10.1023/A:1008651105359