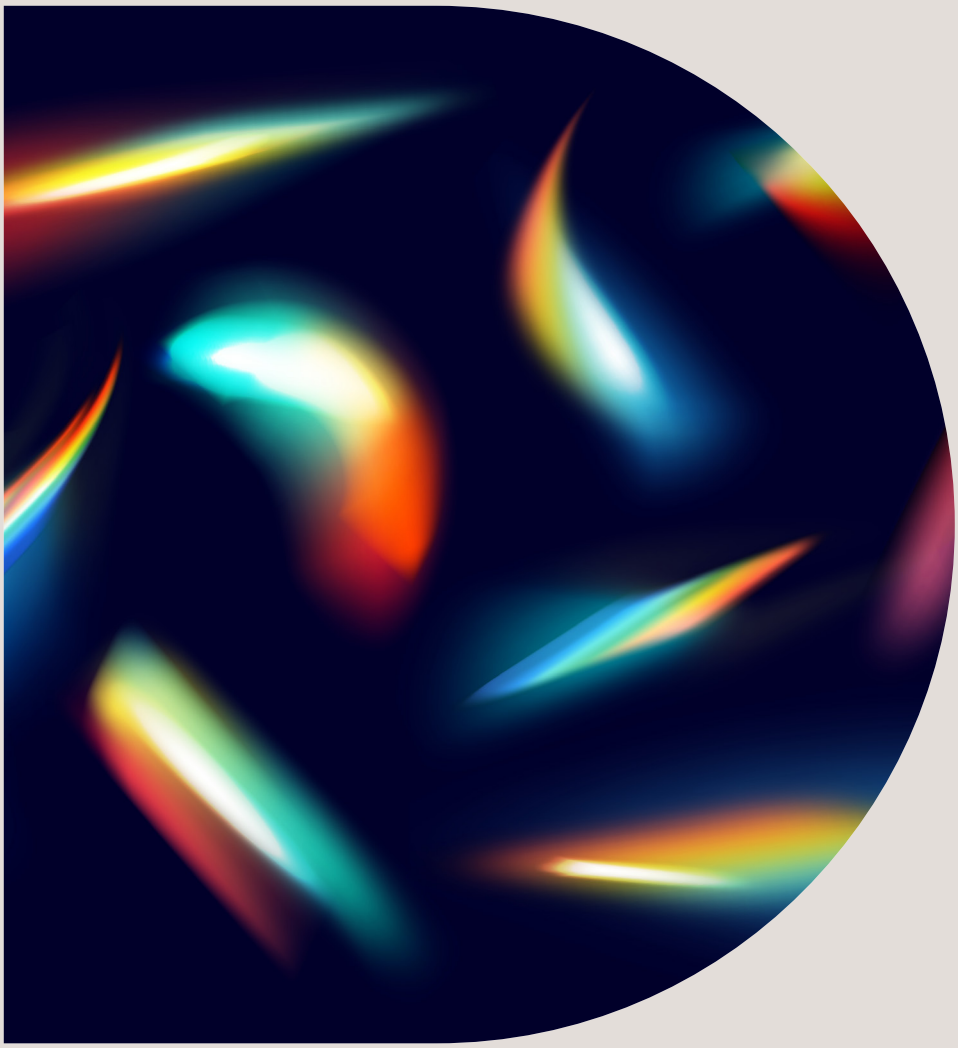
Mainstreaming gender into cyber capacity building

A cyber practitioner's toolkit



Digital Intelligence

BAE SYSTEMS

Summary

The field of cybersecurity is underpinned by numerous gendered assumptions, posing several challenges to the industry itself.

This problem takes on an additional layer of complexity in the context of cybersecurity capacity building (CCB) - international development initiatives that support partner nations' ability to deliver cybersecurity more effectively themselves.

With gender mainstreaming an increasingly core requirement of many cybersecurity capacity building projects, the following questions arise: how can we export cybersecurity expertise in a way that is sustainable, inclusive and does not replicate the gendered and social inequalities embedded in current practices? And how can we create opportunities for positive impact on gender equality?

This paper outlines some simple approaches to designing gender-conscious cyber capacity building initiatives. It follows the development of an internal toolkit to help cybersecurity practitioners apply gender mainstreaming to their work. By breaking the issue down, it provides a way of considering the gendered dimension of cybersecurity not just in terms of equal participation in the workforce, but through designing gender-responsive policy, content, procedures and data to underpin cybersecurity decisions.

Introduction – why are we talking about this?

People use, and are impacted by, digital technologies in different ways. Designing a cyberspace that is secure and stable should therefore account for the different experiences, capabilities, needs and priorities of those using it.

There is a growing recognition that gender considerations have a valid presence in debates surrounding cybersecurity. Understanding how gendered assumptions underpin our cybersecurity activities and objectives is a step towards ensuring that social inequalities are not replicated through cybersecurity programmes. This is important not just for humanitarian reasons; when the needs of certain user communities are neglected, it creates blind spots that can undermine the overall security and resilience of cyber ecosystems. In the long run, addressing the gendered dimensions of cybersecurity offers one solution to the capacity shortages felt across government and industry.

Nonetheless, there is still an overriding failure to "mainstream" these gender considerations into the "core" discussions and decisions at organisational, national and international levels. Part of the challenge is the lack of practical strategies for doing so - 'mainstreaming gender' is often reduced to 'bringing more genders into the room', with a limiting effect to a broader understanding and more impactful interventions.

The aim of this paper is therefore to expand and more clearly define the problem space for cybersecurity practitioners, and suggest some practical approaches for gender conscious cybersecurity initiatives – to the benefit of both an organisation's security objectives, and better welfare for all.

What does it mean to apply a gendered lens to cybersecurity?

Cybersecurity is about people, process and technology.

Cybersecurity is about protecting devices, networks, services and information from technical attacks, harms and breaches, so they are able to perform their intended function.[1] Somewhat simplistically, it is typically thought of as a technology-based problem that has technology-based solutions. Yet in practice, effective cybersecurity depends as much on the people and processes using and being impacted by these technologies as it does on the technologies themselves. As anyone implementing security will know, cybersecurity is more than just a technical problem – it is also a wider security, policy and equality issue that is underpinned by data, priorities, and people.

Cybersecurity capacity building, then, is about developing the ability of other organisations – governments and industry alike – to deliver a nation's collective cybersecurity goals. As the ubiquity of digital technologies across economies, politics and civil society has increased the importance of cybersecurity for the overall stability of nations and wellbeing of their citizens, many of the world's 'cyber powers' are now dedicating significant security and foreign policy resources to this form of cybersecurity-focused international development. This involves partner nations sharing specific cybersecurity expertise through skills and knowledge transfer across the 'people, process and technology' spectrum. Through specific interventions, this aims to improve the ability of partners to develop, implement and collaborate on cybersecurity strategy, policy, legislature, resourcing and services.

The gender dimension

Cyber capacity building presents an opportunity for developing cyber ecosystems in a way that is sustainable – both from a socio-economic perspective, and for the long-term benefit of the industry. From a gender perspective, this opportunity is twofold: on the one hand, it requires us to ensure that the programmes do not reproduce and intensify existing social inequalities. On the other hand, it enables us to scope out possibilities for positive impacts, both in order to improve gender equality and to increase the capacity of organisations delivering cybersecurity.

But, what does this mean in practice? Our mainstreaming toolkit is intended to support practitioners along two dimensions:

- Expand our view of the possibilities for positive impacts beyond participation in the cybersecurity workforce;
- Identify and define a part of the problem space that is feasible to address within the scope of work.

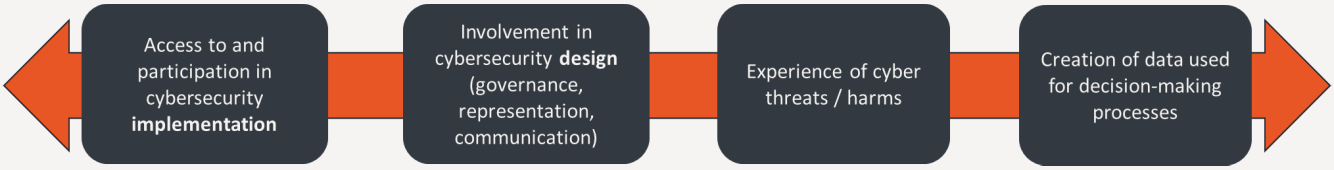
Widening the problem space

We can start thinking more laterally about the problem space, by asking ourselves a simple set of questions:

- Cybersecurity designed and delivered by whom?
- Cybersecurity for whom?
- Cybersecurity that prioritises protecting what?

Deeper probing reveals that our traditional ideas of 'security' – including who delivers it, who is in need of it, and which interests and assets are prioritised – are gendered. Amongst other things, these ideas are based on historic assumptions about the roles and characteristics that men and women occupy throughout societies, and the configurations of structural privilege and structural disadvantage these have given rise to.[2] In cybersecurity these 'gendered' dynamics influence online behaviour and experience, determine access and power, and factor into real or perceived vulnerability.[3]

Gender mainstreaming is the process of taking these considerations to the very core of cybersecurity projects. It involves "assessing the implications for women and men of any planned action across all areas and at all levels" to make "women's and men's concerns and experiences an integral dimension of the design, implementation, monitoring and evaluation" of various cybersecurity programmes.[3] It requires both integrating gender perspectives to the content of cybersecurity programmes, as well as addressing the representation of men and women working on various cybersecurity issues.



Clearly, mainstreaming gender is about more than 'getting more women into the room' which often manifests as counting the proportion of female workshop attendees or cybersecurity teams. Rather, it is about unpacking all the gendered assumptions and dynamics that underpin the design and implementation of cybersecurity. These interventions exist across the spectrum of organisation, people, process, and technology interventions. We have broken the problem space into four areas, which are illustrated above and discussed in depth below.

Cyber threats and cyber harms

Cybersecurity protects information & services, people, organisations and nations from 'cyber threats'. Through conducting 'threat modelling', organisations identify which actors have the ability and intention to cause organisations harm, and which vulnerabilities they may exploit.

Despite being presented as abstract and impartial, this process often draws on a set of assumptions about which impacts organisations are most concerned about, and which threats and vulnerabilities pose a risk to these. This process leads to certain threats and impacts being prioritised over others.

Take, for example, a recent study that found most smart home threat models are set to detect for threats from remote hackers to the user. These same models are not capable of detecting far more prevalent threats to users, such as technology-facilitated abuse from current or former partners.[4] The consequence of this abstract form of threat modelling, is that some groups will have cybersecurity threats that are specific to their community group downplayed to them, or suffer additional security burdens.

A gendered approach adds necessary nuance to this 'top down' methodology. It integrates the diverse experiences of user communities to ensure threat models reflect their variable priorities and needs, enabling the industry to prioritise, research and mitigate against a bigger range of threats for greater audiences. It is a form of threat modelling for humans rather than just systems, and is important for securing the overall stability and wellbeing of society. It can be considered across the following areas:

- Are you collecting data on which types of attack are particularly prevalent amongst vulnerable communities, or how particular forms of social engineering exploit gendered assumptions? Are you collecting disaggregated data on reported cybercrimes e.g. online gender-based attacks such as intrusions or disruption of personal devices?
- Are you considering the downstream impacts of certain forms of data breach, e.g. of medical records, when assessing the severity and priority of incidents? Have you considered resources to protect these vulnerable groups – for example, contingency plans for when the infrastructures they depend on are impacted by cyber-attacks?
- Has your organisation consulted user communities as to their technology requirements, and barriers to technology use and adoption?
- Have you consulted a diverse set of stakeholders that reflects the spectrum of technology uses?

Cybersecurity workforce

This section concerns the people who implement the processes and technologies, and who define the 'in' and 'out' groups. Cybersecurity as an industry suffers from workforce shortages, rendering competition for skills fierce and contributing to the growing digital gap between the public and private sector. In this context, entry barriers for female workforce are excluding a major talent pool that can help solve wider capacity issues.

When we consider the typical IT worker, images of the 'geeky IT guy' who wears a hoodie and is into video games and coding often come to mind.[6] The predominance of these gendered assumptions reflect the lack of diversity in the cybersecurity and IT workforce. This is not just problematic from a gender equality perspective; barriers to the industry are keeping out a huge amount of talent and resource, sustaining capacity issues felt all over the world.[6]

A root cause analysis has linked this to a global digital literacy gap between different gendered communities, including access to technologies and educational opportunities.[7] It has also linked it to the stereotypes and gendered workplace cultures that pervade the industry. Interestingly, the early computing industry was relatively open to women.

Stereotypes affiliating the profession with 'masculinity' only emerged as the industry rose in social prestige through its increasing importance to the economy.[4] Yet these stereotypes and gendered workplace cultures also act as barriers to diverse participation, thus perpetuating the gendered structure of technical cybersecurity expertise, as well as subsequent hiring and promotion practices and the ability to determine policy.

These barriers can be addressed in multiple ways by considering:

- What national-level or organisational education/upskilling initiatives exist, and how much resource are these being given?
- Where are you recruiting from, and are these offering a gender-balanced skills pipeline?
- What barriers to implementation processes are there?
- Are you challenging gender stereotypes, for example through role modelling, networking opportunities and the external presence of your organisation?

Cyber ecosystem design and governance

Building on the previous point, cybersecurity is about more than just the composition of the workforce itself. It is as much a legal, policy and strategy issue as it is a technical one that concerns wider questions about who decides on priorities, what policy is set, and what risks matter most to a nation. It reflects how cybersecurity is prioritised across numerous national policy areas, and the considerations afforded to gender-differentiated impacts.

Once the economic and social role that cybersecurity plays in national wellbeing is recognised, it provides opportunities to widen the scope of objectives to better suit users. This also requires a commitment to giving this issue sufficient resources, governance and coordination in order to be delivered effectively.

Potential considerations include:

- Which ministries, private sector organisations and civil society networks are included in the formulation of cybersecurity strategies?
- Who is setting the cybersecurity priorities, and who are these priorities catering for?
- What steps are you taking to upskill stakeholders, so they are able to participate more effectively to the gender/cyber conversation?
- Which national policies, commitments, and legal frameworks does your strategy draw on and support?

Data to support decisions

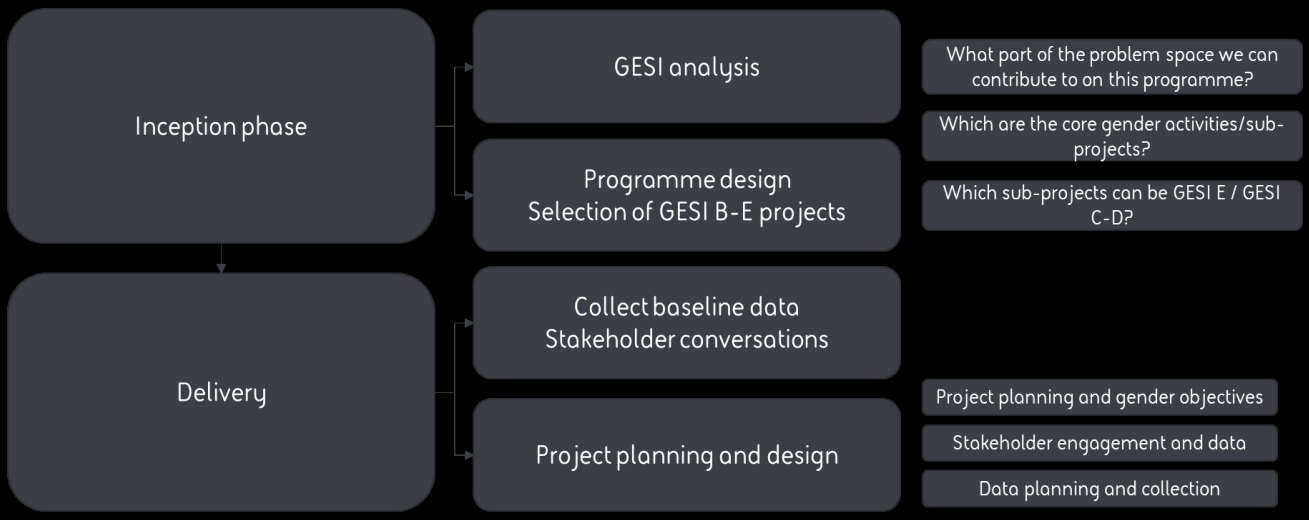
This issue concerns the availability of, and bias contained within, the datasets that underpin our cybersecurity decisions. This includes considering whether disaggregated data is being collected, what assumptions are made in the data's classifications, and in what context the data was produced.

For example, by asking questions about the social, historical or institutional environment under which datasets were produced, the purpose the dataset was created for, and the identity of the people that created it, we can better understand the functional and ethical limitations of a given dataset and whether it is giving us a complete picture. An analogy would be if a pharmaceutical manufacturer only collected medical data of men, pharmaceuticals would only be designed for male health issues and tested against male biology.

The issue becomes clear when we consider, for example, the notion of 'normal user behaviour'.[8] Many security solutions draw on models of user behaviour that are assumed to be standardised, and that do not provide a nuanced view of how technologies are used by different groups in different contexts. For example, users may not be traditional breadwinners that work in 'normal' hours – instead, childcare requirements may require flexible working that security software may flag as 'abnormal' behaviour. In practice, this generates additional and unnecessary security burdens both for users and security staff. Reviewing the data that underpins our cybersecurity practices and decisions is an important component to ensure it better caters to diverse use cases.

Applying a gendered approach to cybersecurity

The previous section captured a lateral view of the problem space in which cyber capacity building is delivered. The second dimension of our gender mainstreaming toolkit aims to assist our cybersecurity practitioners in thinking through how the scope of their cyber capacity building work creates the opportunity to positively impact gender equality. Built on lessons learned from previous CCB programmes, it is broken into a series of steps to make gender mainstreaming a more manageable challenge from the perspective of cybersecurity professionals:



What part of the problem can we address with this scope of CCB work?

During inception phase – specifically the GESI (Gender, Equality and Social Inclusion) analysis – we define what part of the problem space we can feasibly contribute to this programme. The GESI analysis stage researches the context in which the CCB programme will be delivered, and invariably highlights a range of systemic issues in the socio-political and economic context which lead to gender imbalances in all the areas of cybersecurity described above – experience, workforce and governance. It is usually a very large problem space; the challenge is then to identify which part of the problem space is feasible and optimal to address with this scope of work.

What are the core gender activities and sub-projects within this programme of work?

We then identify the degree to which we can create gender-specific interventions as part of a programme, either a dedicated gender project or cybersecurity projects which can be designed or expanded to incorporate a positive gender impact. The expansion of cybersecurity projects to include those gender impacts may form a tangent to the envisaged scope of work. This may involve a trade-off of resources with other programme outputs, and so should be discussed with the programme owner.

Having the stakeholder conversation at a programme level

Where multiple projects, delivered to different stakeholders or different parts of the national ecosystem, will have a gender aspect to them, it makes sense to have the programme-level conversation with senior beneficiaries. Such a conversation places gender in the context of the CCB efforts within the scope of the programme. The reasons for this include both senior sponsorship and coherence. Sponsorship at the senior stakeholder level will enable better buy-in throughout the stakeholder ecosystem. Indeed early conversations may identify 'champions' who can amplify the programme effort and provide traction when needed. Secondly, it enables all subsequent stakeholder conversations about gender objectives of specific projects to refer back to the high level context of the programme gender objectives.

Collect baseline data

If CCB programmes of work aim to deliver gender-positive impact in a particular problem space, then it makes sense to collect baseline data at the start of the programme so that we are well placed to measure the impact that the programme is making. This will naturally feed into the monitoring, reporting, evaluation and learning process, which includes the collection of baseline data. Examples include: the number of women in technical teams; gaps in the gender disaggregated data that is currently available; or current understanding of the gender differentiated impacts of cyber-attacks, and many more.

Design projects that consider the breadth of potential gender impact

Finally, we move into the phase of scoping and designing specific interventions with a gender mainstreaming lens. When scoping a cybersecurity capacity intervention, we should think broadly about the gendered assumptions that underpin each intervention. Within BAE Systems, we have developed an internal framework for considering how types of cybersecurity projects can have a gendered impact, with the intention of challenging ourselves to think more laterally and creatively about gender impact on the full spectrum of cybersecurity interventions. These include the full range of organisation, people, processes and technology projects, including looking downstream and upstream of the work we are delivering. How are these risks prioritised? How are these threat actors prioritised? How are critical sectors prioritised?

Conclusion

Cybersecurity is about more than just using technologies to safeguard our information and services. It's about effectively harnessing human resources to improve the overall security and wellbeing of organisations/societies. The reality is, cyberspace serves different functions and needs for different users. The way it is designed at a programme and project level needs to account for this diversity of experience, behaviours and priorities.

The challenges in mainstreaming gender into cybersecurity capacity building range from programmatic approaches, to the gaps in understanding between cyber practitioners and gender experts. This paper draws on experience from both cyber implementation experience and cyber capacity building, to create a toolkit to help apply gender mainstreaming at a programme and project level. The toolkit incorporates two dimensions – thinking more laterally and creatively about the potential problem space, and taking manageable steps to define the part of the problem space to address within a particular scope of work.

By sharing experiences of what works, and what has not worked, we will continue to work with the cyber capacity building community to build our collective competence in this domain.

Reference List

[1] https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[2] https://data-feminism.mitpress.mit.edu/

[3] https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

[4] https://www.oii.ox.ac.uk/wp-content/uploads/2021/01/Reconfigure-Report-v6-pages.pdf

[5] https://blogs.worldbank.org/governance/governments-arent-getting-enough-digital-skills#_ftnref1

[6] https://www.oii.ox.ac.uk/news-events/news/challenging-gender-stereotypes-in-cybersecurity-a-feminist-perspective/

[7] https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf

[8] https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

BAE Systems, Surrey
Research Park, Guildford,
Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

BAE SYSTEMS