OFFENSIVE CYBER WORKING GROUP

Crafting a democratic and responsible cyber power?

Workshop Report, August 2022

Offensive Cyber Working Group

Written by Andrew C. Dwyer

Executive summary

- A workshop exploring democratic and responsible cyber power was held at CyCon in Estonia in May 2022 to explore its different, and often competing, dynamics.

- Participants at the workshop displayed a highly contextual interpretation of cyber power dependent on the activity and focus:

    - When scoping cyber power, participants tended to emphasise the continuing and enduring reliance of cybersecurity more commonly as well as a focus on the promotion of a state's projection of social, political, and cultural values.
    - During prioritisation of the aims of cyber power, participants tended to focus on its 'harder' elements, state-centric policies, including intelligence collection and offensive cyber capabilities.
    - A final definitional exercise promoted the concept of cyber resilience and emphasised cyber power as another form of national power among others.
    - When cyber power was applied to states with limited cyber capabilities, there was a greater focus on the cyber ecosystem, partnerships, and diplomacy.

- Despite the workshop addressing both *democratic* and *responsible* cyber power, participants tended to focus on responsible governance, rather than on its democratic attributes. This suggests that participants did not see an explicit link between what may be understood as responsible behaviour and whether this needs to be achieved through democratic means.

- Participants worked with three fictitious case studies with less developed state cyber capabilities. This presented a different focus from more abstract notions of cyber power and instead turned to attention to the cyber ecosystem, partnerships, and diplomacy. This is demonstrative of how cyber power is highly contextual and appeals in different ways according to context, audience, and capability.

- Cyber power, as a concept, due to its varying – and contextual – interpretations, should not be understood as a common framework. Rather it is a range of practices and concepts that can be used as an ordering concept for different actors to explore the contours of how computational networks, processes, and power are transforming the dynamics of state power.

- Future research may focus on the distinctions identified in the application of cyber power for different states and whether a focus on an expanded conceptualisation of responsibility rather than on the 'democratic' may hold greater applicability and meaning for a variety of states and communities.

Introduction

Computational networks have become one of the, and if not the most, defining features of the contemporary period, enabling sustained economic and social development as much as transforming every day and banal interactions. Insecurities and vulnerabilities have, however, accompanied such a transformation[1], where states have sought to address such concerns through varying cybersecurity strategies and their attendant development in policy and delivery. Yet, despite 'cybersecurity' being an organising concept to conceptualise and operationalise responses to computational (in)securities in the past decade or so, this no longer appears to be sufficient for some states to address their identified geopolitical, technological, and societal challenges ahead. Partly, this attends to the increasing volatility on the international stage, currently in Russia's invasion of Ukraine, as much as China seeks to challenge the European and North American dominance of technology and long-term power balance through exploitation of technologies and more assertive foreign policy[2].

Recently states, primarily in the 'west', have sought to expand the scope and range of interventions they can make that address the changes that computational processing, networks, and standards have made. For some, this has increasingly solidified in strategic thinking around 'cyber power'. Although the term has a longer history in military and academic thinking[3], only more recently has cyber power come to represent, and be, an organising concept to deliver a 'whole-of-society', or 'whole-of-nation', approach to ensuring security and projection of power on the international stage. This development has come alongside the growth of more assertive and organised capacities in offensive cyber capabilities through state cyber forces that have increasingly proliferated[4], and which members of the Offensive Cyber Working Group have previously co-written a report with King's College London on the UK's National Cyber Force[5].

The expansive scope of cyber power is arguably intended to incorporate an ever-increasing expanse of different national security priorities. For example, the UK's 2021 Integrated Review of Security, Defence, Development and Foreign Policy ('IR')[6] and its National Cyber Strategy 2022 ('NCS')[7] outline its position on, and interpretation of, cyber power. As the UK NCS defines on p. 11, "[c]yber power is the ability to protect and promote national interests in and through cyberspace." This includes, for the UK: conventional concerns of cybersecurity; cyber resilience; improving the cyber ecosystem including the development of skills, increasing investment and advancing technological innovation; building industrial capacity and sovereign capabilities; the UK promoting its national interests in foreign policy, negotiating beneficial international technical standards; international capacity building and development; to ensuring a capacity for offensive cyber operations.

Cyber power, when inclusive of all the above, and more, then becomes difficult to disentangle from a modern interpretation of power through computational means. At least from the perspective of the UK, it is not just about security of computation, but about securing the

[1] Parikka, J., & Sampson, T. D. (2009). The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture. Hampton Press.
[2] Segal, A. (2018). When China rules the web: Technology in service of the state. Foreign Aff., 97, 10–18.
[3] Nye Jr, J. S. (2010). Cyber power. Harvard Univ Cambridge MA Belfer Center for Science and International Affairs.
[4] Smeets, M. (2022). No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. C Hurst & Co Publishers Ltd.
[5] Devanny, J., Dwyer, A., Ertan, A., & Stevens, T. (2021). The National Cyber Force that Britain Needs? King's College London.
[6] HM Government. (2021). Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy. HM Government (UK).
[7] HM Government. (2021). National Cyber Strategy 2022. HM Government (UK).

international rules-based order, and challenging what it deems as strategic competitors. Although one may acknowledge that many states engage in alternate forms of cyber power, the UK hinges its being both *responsible* and *democratic* in nature. This is in order to distinguish itself from the likes of China, Iran, North Korea, and Russia as well as offering a clear brand and niche for the UK[8] in comparison to some critiques of the United States' more assertive cyber power ambitions.

The pursuit of cyber power also must address the more assertive and divergent uses of offensive cyber capabilities by states; and one way in which cyber power has been conditioned and understood by states such as the UK is to emphasise both *responsibility* and to bring together ideals around *democratic governance* to the fore[9]. However, it is unclear how and what responsible and democratic cyber power could mean to various audiences and the tensions that may emerge in framing cyber power in such a way.

Therefore, the Offensive Cyber Working Group delivered a workshop to explore what democratic and responsible cyber power is, partially derived from the UK's thinking and discussion on the topic. This was conducted across three primary themes: First, scoping out the possibilities of cyber power; Second, articulating the priorities for cyber power, and; Third, applying cyber power 'beyond the usual suspects' to three fictitious case studies. This produced a complex picture and narrative to the context of both democratic and responsible approaches to cyber power. At each stage there were varying interpretations and developments, with participants tending to focus on the 'harder' elements of cyber power, such as intelligence collection and offensive cyber operations when talking abstractly. However, when applying cyber power was being broadly scoped or applied to case studies with less developed state cyber capabilities, participants identified cyber power's 'softer' elements, including the enduring importance of security and the promotion of values as well as ensuring a strong 'cyber ecosystem'.

This workshop report then offers an analysis and interpretation of an event held at CyCon in 2022, and proceeds by following the workshop's structure across two sessions that participants were engaged in. First, asking what cyber power is, and second, how cyber power beyond the usual suspects could be applied to three fictitious case study states. In the next section, the workshop is outlined in greater detail, before continuing to describe and analyse how participants scoped, prioritised, and defined cyber power, and how cyber power looks to states beyond the usual suspects to explore the details of what it may mean to be both democratic and responsible.

[8] Shires, J., & Smeets, M. (2021, November 23). The U.K. as a Responsible Cyber Power: Brilliant Branding or Empty Bluster? Lawfare.

[9] For example, see President Biden's Summit for Democracy initiative for a non-UK example and for a discussion the UK's recent legal position regarding offensive cyber operations, see Dwyer, A.C. and Martin, C. (2022). A Frontier Without Direction? The U.K.'s Latest Position on Responsible Cyber Power. Lawfare.

The workshop

The workshop – "Crafting a democratic and responsible cyber power?" – was advertised in advance to attendees of the International Conference on Cyber Conflict (CyCon) held in Tallinn, Estonia and organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Conducted on 'Day 0' of the conference on May 31, 2022 (1300 – 1700 EEST), there were thirty-six individuals[10] who took part from both NATO and non-NATO states: with the greatest number of participants from the USA. This was led by Andrew C. Dwyer, with extensive facilitation support from Neil Ashdown, Nicola Bates, and Louise Marie Hurel curated through the Offensive Cyber Working Group. The workshop was intended to offer participants either time to reflect on their own state's cyber power or for capacity building for participants from states who may be exploring what cyber power may mean for them.

The workshop was conducted under the Chatham House Rule[11] and consisted of four components under two sessions separated by a tea break. First, an introduction and invited presentation by Dr. Joe Devanny from King's College London on cyber power; Second, a session 'Exploring Cyber Power' that tasked participants with identifying 'what is cyber power?' and 'what can you 'do' with cyber power?'; Third, a case study session on 'Applying Cyber Power' to develop policy responses for fictitious case study states, before; Fourth, a session on 'Socialising Cyber Power' that shared the case study and involved some conclusions and reflections on the definition of cyber power. Each facilitator supported two groups of around 12 individuals, supporting conversations, and writing notes that informed the production of this report.

In advance of the workshop, attendees were provided with one of three fictitious case study countries to facilitate discussion in the session, 'Applying Cyber Power'. Each case study was purposefully created to avoid discussion of 'great cyber power' competition, typically concerning China, Russia, and the USA. Instead, by providing fictitious case studies, one each based in central Europe, central Africa, and the Indo-Pacific, participants were able to use some of their knowledge of the different areas but avoid devising policies that states use, such as the USA's persistent engagement[12]. This gave freedom to participants to experiment with the case studies as well as carefully thinking through the different components of cyber power as they may apply in contexts unfamiliar to them.

All the materials within this document have been anonymised and do not reflect the opinions of any singular participant.

[10] This is an approximate figure as some individuals did not attend the whole of the workshop.
[11] https://www.chathamhouse.org/about-us/chatham-house-rule
[12] Schneider, J. (2019). Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. Lawfare.

What is cyber power?

Key Take-Aways:

- Broadly scoped, cyber power has a wide-ranging remit with themes that centre on the enduring promotion of (cyber)*security* as well as the promotion of social, political, and cultural *values*.
- When prioritised, the focus of cyber power centred on the economy and resilience as well as the 'harder' elements of cyber power, including the capacity of the state to collect intelligence and to conduct offensive cyber operations.
- There is no singular definition of cyber power; but a focus on security, resilience, and the promotion of values and influence were common.

Following a presentation of cyber power by Dr. Joe Devanny – with a primary focus on the UK's branding in "responsible and democratic cyber power" – participants engaged in a range of exercises to consider what cyber power is. This included a scoping exercise using 'post-it' notes, the prioritisation of key elements of cyber power, and at the end of the day, a final definition exercise.

Scoping Exercise

In the first substantive session, each group was encouraged to maintain an open conversation, exploring divergences and scope the concept of cyber power. Participants offered different elements of cyber power written on post-it notes, as well as using flipchart boards, to discuss what cyber power is, or could be. Towards the end of this session, each group was tasked to select their 'top 5' to present back to the workshop. **Error! Reference source not found.** is a visual representation – a 'word cloud' – of the themes from the analysis of the top 5 post-it notes from all the groups[13]. In this process, two dominant themes emerged. These were the promotion of social, political, and cultural ***values*** as well as the emphasis given to the enactment of the (cyber)***security*** of the state, organisations, and citizens. Other common themes included the protection of ***critical national infrastructures*** (CNI), the importance of ***international law*** to the governance and potential of cyber power, ***deterrence*** as key motive to promote cyber power, as much as how ***private enterprise*** (part of the cyber ecosystem) enables and constrains cyber power (such as in the development of new technologies and their ownership of infrastructure).

The dominance of the ***security*** and ***values*** suggests that in a broad scoping of cyber power, it is both the conventional enablement of cybersecurity as well as the expanded scope of cyber power to promote of certain values (whether these are democratic or not) that are key. Therefore, in this scoping exercise, participants tended to understand cyber power as dependent on both strong security and promoting values that adhere with the ambitions of states and communities. This suggests a continuity from prior iterations of cyber strategy – through cybersecurity – and the influence of a newer perspective that is about values, which could be democratic or not. Such a combination could be understood to support more enduring forms of deterrence (both direct and indirect) through private enterprise, international law, and securing CNI rather than the 'harder' components of cyber power that often attract greater attention, such as offensive cyber

[13] This used an inductive coding framework by the author, using the post-its to code and thus create categories. Some post-its had multiple codes associated with them.

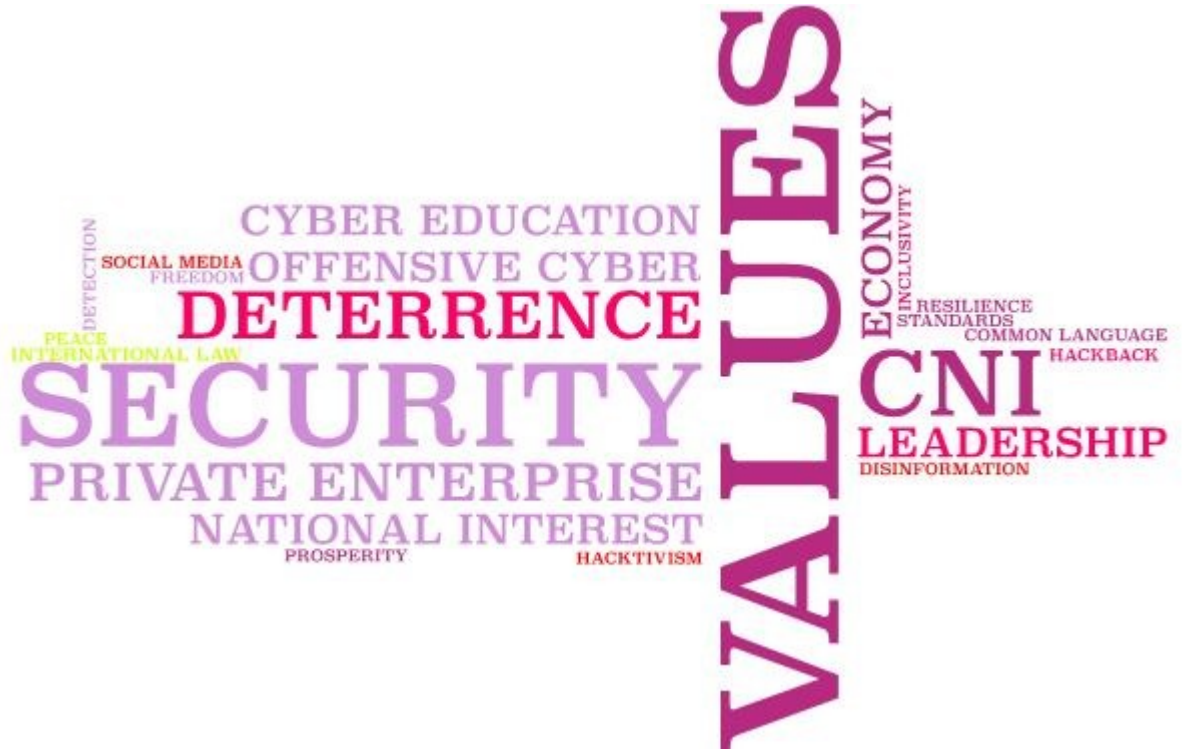

Figure 1: A 'word cloud' of understandings of cyber power. This uses coded data from the 'top 5' post-its produced by each group, with further details provided in Table 1 in the Appendix.

operations[14]. However, as the next activity of the workshop demonstrates, this focus on security and values then changed during prioritisation.

Prioritisation

At the end of the first substantive session, each group's top 5 post-it notes were collected and brought to the front of the workshop room. Each participant was provided with three coloured stickers to stick to post-it notes that they thought best summarised the key elements of cyber power. This process resulted in a selected top 5 post-its:

1. "Collect intelligence: Steal secrets and provide policy decision advantage."
2. "Deterrence of bad behaviour: Through standards, common language, and guidelines."
3. "Maintaining a robust and strong IT sector."
4. "Digitally enabled and resilient society, including secure infrastructure."
5. "Conducting cyber operations on other states."

Each of the top-rated elements of cyber power can be simplified as **intelligence collection**, **deterrence**, **cyber ecosystem**, **cyber resilience**, and **offensive cyber capabilities**. Compared to the scoping exercise, this presents a noted change in tone. The prioritisation by the workshop participants continues with a focus on the role of a strong economy and resilience (including CNI), yet there is a much greater focus on intelligence and miliary matters, including offensive cyber capabilities. This may suggest that, even though there is a potential for a wide focus of cyber power under security and values; when prioritisation is required, participants tended towards to focus less on values and increase the prominence of 'harder' elements of state cyber power that were relatively minimal in the initial scoping exercise.

[14] Note: Dr. Devanny's presentation, which covered the wide axes of cyber power, primarily drawing on the case of the UK Government's "responsible and democratic cyber power" may have influenced participants thinking.

Although this is one workshop, this may be suggestive of required further research, to understand how and why there is a stronger preference for matters that the state can directly control (such as intelligence collection and offensive cyber operations) over the broader matters that were covered during the scoping exercise and require greater collaboration between a myriad of actors. This may reflect the audience (dominated by current and former state employees) or may be that there are limits to the prioritisation of focus in cyber power. Even though cyber power may include the broader remit as identified in the scoping exercise, there is a limit to what states can prioritise, suggesting that for all the expansive notions of cyber power, it may not be all that different to the conventional pursuit of cybersecurity that has historically focused on the technical domain rather than on sociotechnical, political, and cultural matters.

Definitions

At the end of the workshop, each group was asked to produce one collective definition of cyber power, listed in Table 1. One emergent theme across the workshop was the focus of (cyber) resilience. One group explicitly stated in their feedback that the workshop discussions had prompted thinking on resilience. This was not explicitly referred to in either the presentation by Dr. Devanny or the organisers, but appears in three of the final definitions. However, what is also notable is how cyber power is "another instrument of power", the "capabilities to influence", as well as "to protect and promote national interests." That is, cyber power is a function of national power rather than expressly relating to technological capabilities. These final definitions focus heavily on the capacity of resilience as well as ensuring "influence". This should not be ascribed to the earlier discussed "values" as influence could include both 'hard' (e.g., offensive cyber operations) and 'soft' (e.g., diplomacy) power. Therefore, when producing a *singular* definition of cyber power, there is an indication of a hardening of what cyber power to be through the capacities of states to exert national power through improved "resilience" across different levers of "influence". Sometimes these are state-centric, whilst others are orientated towards societal concerns.

Table 1: A lightly edited list of the 'final' definitions of cyber power from each group at the end of the workshop.

Having the secure and resilient foundations to build, and develop, capabilities to influence cyberspace.
Cyber "power" is another instrument of national power to be weirded when appropriate to secure national objectives, security, prosperity, etc. It is another tool in the toolbox.
Cyber power is the ability to protect and promote national interests in cyberspace.
Cyber power is the combination of security, resilience, defence, surveillance, offensive and influence operations, as well as the international rules-based order.
Cyber power is the exercise of societal resilience through, and with, the cyber domain.
The ability to establish availability and intent through influence and inter-dependence.

Cyber power beyond the usual suspects

Key Take-Aways:

- The most common focus in the application of cyber power to three fictitious case-study states was on the cyber ecosystem.
- Other important elements across the three case studies were the promotion of education and skills, diplomacy and partnerships, and improving state organisation (such as setting up national cyber security centres).
- When states are without significant capabilities in state cyber capabilities, cyber power is less concerned with its 'harder' elements, and participants focused on broader development and cyber capacity measures.

In the second substantive session of the workshop, each group was provided with one of three fictitious case studies. These did not attempt to replicate one of the 'usual suspects', such as China, Russia, or the USA. This was intended to reduce participants' biases and to seek a more neutral starting point to facilitate open conversation and explore the contours of what cyber power may mean in contexts where states had fewer intelligence and offensive cyber capabilities. The case studies were, however, located in real region to enable for a grounding of the geopolitical interactions of the fictitious states. These were, in summary:

1. **Alphaland**: a medium-sized state in southeast Asia,
2. **Blueland**: a large country in central Africa, and
3. **Ruritania**: a small country in eastern Europe.

Each case was no more than three pages long, with most participants being sent material to read in advance, with time within the session for participants to (re)engage with the case study.

Participants were tasked as 'consultants' for each case study state. This required a negotiation of the often-difficult priorities and complexities of the state's foreign relations, resources, skills-base, as well as geostrategic location. Through this process, what emerged was a much more nuanced and widened view of cyber power as it became practically applied, in comparison to the abstracted definitional work in the first session. In the appendix, Table 3

Table 3 lists the recommendations provided by each group. Each recommendation was given one primary code to assess its priorities, which are outlined further in Table 4, also in the appendix.

The most common recommendation across the case studies concerns the ***cyber ecosystem***, or the economic and technological development, of a state. This is followed by another four most common themes: ***education, research, and skills***; ***international diplomacy***; ***partnerships***; and ***state organisation***. These are substantively different to the deployment of offensive cyber operations, deterrence or intelligence collection that were prioritised by participants in the previous session. Thus, here there is an evolution of cyber power orientated to enabling, arguably, forms of cyber capacity building with countries with less development of intelligence or offensive cyber capabilities, rather than a projection of power that is commonly associated with the term by western states. Thus, the recommendations of the groups emphasise consensual working – through international diplomacy and partnerships – in support of strong ecosystems with improving skills through education, all supported by efficient and effective state organisations in support of these objectives (whether that be through establishing 'National Cyber Security Centres' or in establishing a cyber diplomacy corps).

When communicating about cyber power among different states, responsibility tends not to refer to the use of offensive cyber capabilities (although this may pervade international debates). Rather, participants emphasised equally important, if not more banal, elements of cyber power that must be conditioned and contextualised around often more pressing matters of ensuring a stable economy, conventional geopolitical threats, and developing stronger institutions. Responsible cyber power in this context may also be one that acknowledges the limitations of certain types of cyber activity for a state to engage in, how it engages with different communities, and ensure that people feel secure in a plurality of different ways.

Below, the case studies are presented in greater detail alongside an analysis of the recommendations for each.

Alphaland

This case study covered a relatively prosperous economy, based on low-cost electronics manufacturing in south-east Asia with 2.1 million people, with immigration from China. It stated that it had an enthusiastic use of social media, had concerns over disinformation, and a military that was disbanded in the 1990s, replaced with a self-defence force. The state had limited capabilities and nascent efforts in cyber capability. The case study also noted an ongoing maritime dispute and a shared land border with 'Bravoland', with submarine cables and shipping lanes running through disputed waters.

The recommendations from participants prioritised the capacity of the country to keep investing in its ***cyber ecosystem*** as well as developing its ***state organisation***, including the creation of a national cyber security agency. This is reflective of building foundations to cyber power capacity as well as strengthening its economy away from its low-cost electronics base. Participants on this case study also were the clearest on enabling democratic privacy debate and discussions. The case study's outlining of disinformation led to discussions on boosting research, communications campaigns, as well as developing a new intelligence model.

Ruritania

This case study focused on a republic formed out of the collapse of the Soviet Union. This state had sought to balance itself between the West and Russia, but this balance had become strained since the invasion of Ukraine. It is landlocked with a burgeoning services sector with a young tech-savvy population. A flagship business is a threat intelligence and anti-virus company. It is also a key node in regional telecommunications networks with substantial foreign investment in

infrastructure. Its military had participated in US-led operations in Afghanistan and Iraq and seeks interoperability with NATO. It established a signals intelligence service in the 1990s, with significant western support, but this had been questioned on its costs and benefits.

Participants who studied Ruritania focused on the value of ***partnerships*** more than any other topic. This is likely due to its already deep prior engagements with the US and NATO and its geographical position next to Russia. This focuses on deepening strategic cooperation for strategic autonomy, developing regional and multilateral agreements, as well as enhancing partnerships with NATO and improving information exchange. Likewise, there was emphasis on increasing resilience, protecting CNI and utilising its infrastructural position as a telecommunications node.

Blueland

This state was a large country in central Africa, becoming a republic in 1990s after a Marxist dictatorial regime, and had become a western-facing country. There is tension with its neighbour, 'Redland', over the attention given to Blueland by the west that have neglected Redland's own historically strong ties. It mainly exports metals with the potential to be a satellite launch site but is landlocked and is dependent on neighbours for telecommunications and goods access. It has a limited landline network with most of the population using Chinese-made smartphones. It has experimented with blockchain and other digitalisation, but there have been concerns over data sovereignty raised. Its intelligence agency is above average for the region and has a nascent digital surveillance capacity.

The analysis of Blueland by participants gave a wider distribution of priorities than for Alphaland and Ruritania. These included improving its ***cyber ecosystem***, addressing ***education, research and skills***, as well as ***capacity building***. This is demonstrative of the multiple competing objectives of what participants believed were the core requirements for cyber power. Like the other two case studies, the improvement of the cyber ecosystem was important, but so was attracting funding and donors and borrowing western frameworks for capacity building[15]. Key was also enhancing cyber literacy for citizens.

What the different case studies demonstrate, then, is that when cyber power becomes applied to states that do not have significant capacity for intelligence or offensive cyber capabilities, participants tended to draw on the broader topics identified in the scoping exercise. Yet, the common denominator across the three case studies was the need for a strong cyber ecosystem. This is perhaps reflective of the private nature of much of the applications and materials of cyber security, which participants most identified in the scoping exercise alongside values. Thus, without a strong cyber ecosystem, these case study states would be unable to pursue other forms of cyber power without it.

[15] For a critical account of the role of cyber capacity building, see Hurel, L. M. (2022). Interrogating the Cybersecurity Development Agenda: A Critical Reflection. The International Spectator, 57(3), 66–84.

Conclusions for cyber power

Key Take-Aways:

- Participants identified responsible behaviour for cyber power across the workshop, and most discussions within groups tried to balance competing priorities for states.
- Democratic cyber power was referred to in limited instances, with workshop participants often talking about better governance models that do not necessarily equate to democratic processes.
- Based on the workshop, further research may wish to engage with how responsibility may interlock with democratic processes, but not be equivalent with the latter.

Throughout the workshop, a variety of interpretations of cyber power were given according to the context of the application. Therefore, cyber power does not have one definition or interpretation. Within the workshop, participants were asked to: 1) scope cyber power; 2) prioritise definitions from the scoping exercise, then; 3) to act as consultants and apply cyber power to a given case study fictitious state. Each section produced different configurations of cyber power.

On the dimensions of what *responsible* cyber power is, there was much discussion and reflection. It was also often discussed with regards to the *responsibility* of states to their citizens, communities, as well as the international community, rather than what is typically a more restrictive debate in the UK and elsewhere over the responsible use of offensive cyber operations. For example, it included balancing competing priorities, the extent to which offensive cyber operations should be deployed, to developing common frameworks and international norms. This may suggest that when discussing *responsible* cyber power, there is scope to speak in more expansive ways to speak about governance, economic development, and more.

Yet, little, if any, of the participants generated explicit perspectives on what a *democratic* cyber power may be. Although there was discussion about increasing participation in society for cyber power (e.g., around skills and increasing resilience); this should not be confused with, and connected to, democratic participation and practices. The closest that participants came to discussing democratic processes came in one Alphaland group who promoted discussion of privacy protections as well as one suggestion during the scoping exercise to democratic freedoms. Participants did not then explicitly connect both democratic and responsible together when discussing cyber power. Rather, there was a determined focus on responsibility and the pursuit of state power.

Articulating *democratic* cyber power may require further development and thought. Indeed, as Prof. Joanna Weaver[16] noted at a CyCon keynote later in the conference, most states are not democratic, and participate in developing norms and a rules-based order to secure their own power rather than to ensure democratic practices. The lack of democratic discussion at the workshop then suggests that to be responsible is then not expressly tied to democratic processes. As much as cyber power may be responsible through the promotion of democratic practice, responsibility can also emerge in non-democratic practices. The workshop then suggests that may be a 'middle ground' to be found that focuses on responsibility (that could be participatory), where states could achieve this through democratic processes and norms. However, there appears to be little consensus that this is required for the promotion of cyber power. Indeed, certain

[16] Weaver, J. (2022). "The Rules-Based International Order: some hard truths". CyCon: 1 June 2022.

elements of cyber power may sustain and promote certain authoritarian practices and governance models.

Drawing on the participants' contributions, it is then difficult to assess *what* democratic and responsible cyber power together is. Cyber power could be summarised as an ordering concept that bring together a collection of different elements of national power that are reliant on computational connection: whether in their direct exploitation, in developing new technologies and skills, as well as working with other states through diplomacy and partnerships. As computational technologies have become increasingly interwoven into contemporary societies, however, it may become difficult to distinguish cyber power (if this has ever been possible) from other sovereign power aims and objectives for states.

In summary:

- When scoping cyber power, there is an emphasis on the continuing and enduring reliance on the centrality of cybersecurity as well as a newer focus on the promotion of a state's social, political, and cultural values.
- During prioritisation, participants tended to focus on the harder elements of cyber power, including intelligence collection and offensive cyber capabilities, suggestive of a tighter scope on state-centric capabilities when there are a limited number of options.
- Definitional exercises promoted the concept of cyber resilience and emphasised cyber power as another form of national power.
- When cyber power is applied beyond the usual suspects, there is a greater focus on the cyber ecosystem, partnerships, and diplomacy.

The different emphases according to the exercise then suggest that participants were flexible over the concept of cyber power, and means when discussing cyber power, it is essential to understand the context in which it is used and according to which states and communities people come from.

Appendix

Table 2: The codes, descriptions, and number of times each code was used. Some post-its had multiple codes associated with them.

Code	Description	Number of Post-its
CNI	Critical National Infrastructure.	4
Common Language	Reference to a 'common language' across different actors and institutions.	1
Cyber Education	Any mention of improving education and capacity of citizens to act.	2
Detection	Referencing capacities to detect adversary behaviour.	1
Deterrence	Deterring adversaries from engaging in hostile behaviour.	3
Disinformation	Limiting the distribution of disinformation online.	1
Economy	References to economic incentives or considerations	2
Emerging Technologies	Consideration of new technologies and how they may change outcomes.	1
Freedom	The promotion of democratic freedoms	1
Hack back	A capacity to hack adversaries if one has already been hacked.	1
Hacktivism	Non-state actors hacking on behalf of a state.	1
Inclusivity	Including citizens in developing cyber power.	1
Intelligence Collection	Any form of intelligence gathering and collection.	2
International Law	Any mention of international law.	4
Leadership	The explicit mention of a state promoting itself.	2
National Interest	Referring to strategic national priorities and self-interested gains.	2
Offensive Cyber	Reference to the conduct of cyber operations.	2
Peace	Promotion of peace in cyberspace.	1
Private Enterprise	Any reference to the support, or contribution of, the private sector.	3
Prosperity	Improving the prospects of the state or citizens.	1
Resilience	Improving the capacity of a state, organisation, or citizen to respond.	1
Security	The performance of functions to improve the capacity of a state, organisation, or citizen to defend itself.	7
Social media	Reference to social media platforms.	1
Standards	Reference to technical standards or norms.	1
Values	Social, political, or cultural attributes that the state wishes to promote.	7

Table 3: Recommendations from each group during the case study exercise, with some light editing for clarity.

Group	Case Study	Recommendation 1	Recommendation 2	Recommendation 3	Recommendation 4	Recommendation 5
1	Alphaland	Join ASEAN security working groups	Boosting academia with funding from aligned states	A "fact checking" communications campaign	Privacy debate and protections	Boost the IT sector
2		Develop secure infrastructure	Create a National Cybersecurity Agency	Create Special Economic Zones (SEZs)	New intelligence model (separation between foreign and domestic capabilities)	Subsidize domestic IT industry (competition with Chinese imported services)
3	Ruritania	Strategy of cooperation to achieve strategic autonomy in cybersecurity, with relevant actors	Invest in resilience and redundancy in national critical infrastructure	Regional/multilateral agreement to leverage resources for national priorities	Create a cyber diplomacy cadre / policy to defend, protect, and promote Ruritania's interests	Write a national cybersecurity policy and implement
4		Exploit Information Position (key node in telecommunications network)	Resilience (implement strategic guard from cyber-attacks and reduce dependence on Chinese technology)	Partnerships (NATO exercises, information exchange)	Influence Projection (use social media to maintain unification and create national identity)	Industry (tech-savvy population with experience in cyber – can provide international services)
5	Blueland	Improve cyber literacy	Improve foreign direct investment	Borrow frameworks from Western states	Development of tech sector to avoid dependence on other states.	*N/A*
6		Infrastructure / satellite (capable for lunches, PPP)	Funding / donors (determine partners)	Expertise/Skills (civilian/military)	Regulation (e.g., data protection)	International cooperation

Table 4: Coded analysis of recommendations during the case study activity.

Code	Description	Frequency
Capacity Building	Refers to improving the capacity of a state's cyber security; whether through frameworks or funding.	2
CNI	Direct recommendation to improve critical national infrastructures	2
Cyber Ecosystem	Referring to building technological capabilities, building industry, and supporting functions to grow the economy.	6
Cyber Resilience	Explicit reference to building resilience as the primary goal of the recommendation	1
Data Privacy	Referring to improving debate of privacy and/or data privacy regulation and laws.	2
Domestic Media	Trying to limit disinformation and/or using social media to promote a state's interests.	2
Education, Research, and Skills	Any reference to the enhancement of education, research capacity or skills.	3
Infrastructural Position	Reference to the capacity of a state to leverage its geographical location and/or position as a critical information node.	2
International Diplomacy	Highlighting international relationships or cyber diplomacy which do not require formal partnerships or alliances.	3
Partnerships	Creating alliances or ties to develop cyber power with other states.	3
State Organisation	Reference to how the state organises itself.	3

Acknowledgements

Thanks goes to all the participants who took part in the workshop for giving up their time and enthusiastically sharing their ideas at Day 0 of the International Conference on Cyber Conflict (CyCon). Further thanks go to the support and generosity of the conference, in particular to Taťána Jančárková and Ingrid Winther, for their dedication and commitment to hosting the workshop as well as the hard work of the three facilitators on the day: Neil Ashdown, Nicola Bates, and Louise Marie Hurel. The three case study materials were also kindly written by Neil Ashdown.

Published by Durham University, on behalf of the Offensive Cyber Working Group

ISBN 978-0-907552-28-4