The Role of the Military in Cyber Power

Digital Intelligence

BAE SYSTEMS

1 Positioning of Cyber Power in the military context

What is Cyber Power?

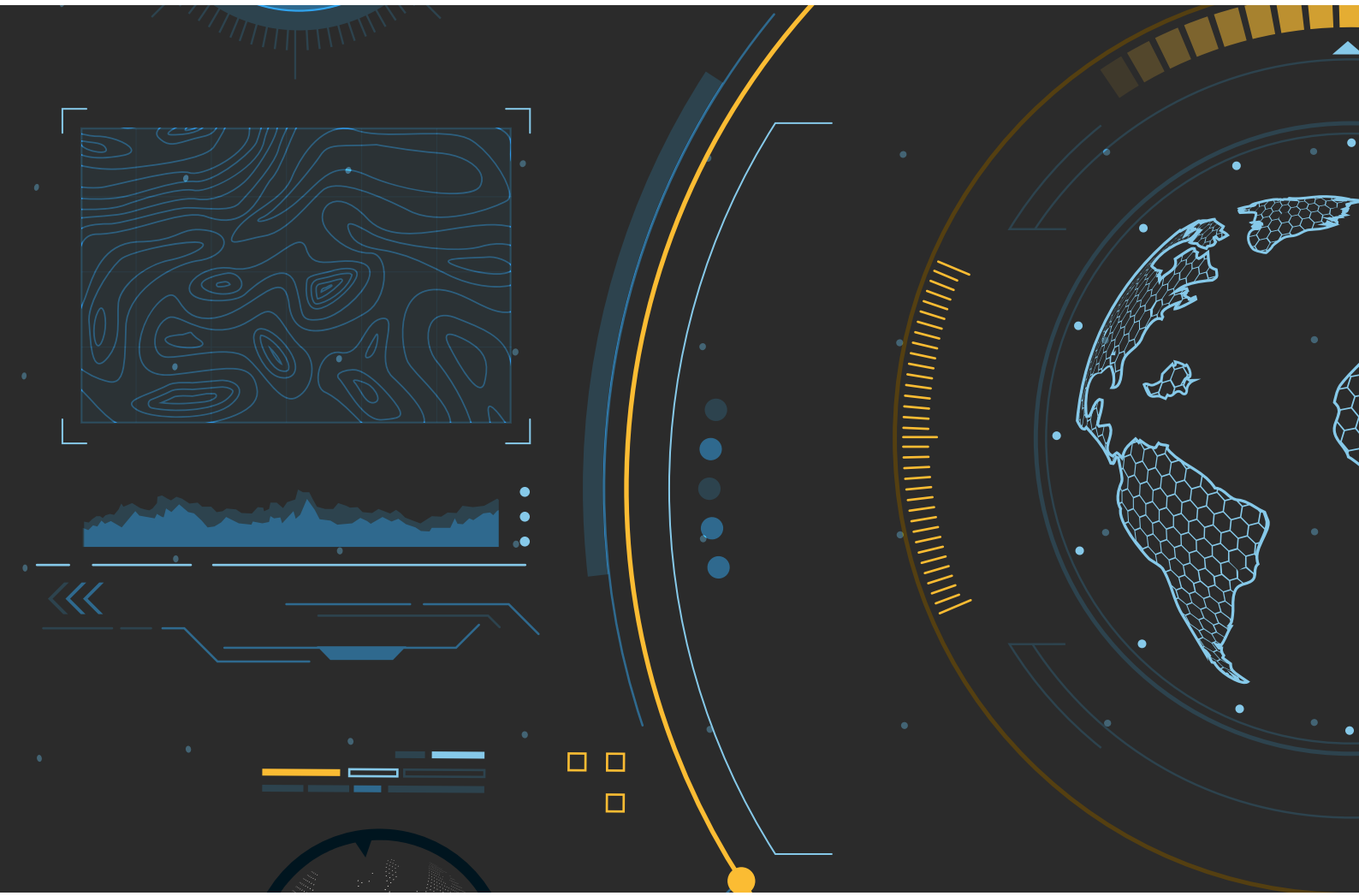
Cyber Power is the capacity to project and promote national interests in and through cyberspace. The real world outcome of this extends beyond defensive activities into the offensive domain, both for purposes of "defending forward"[1] and also for aggressive acts (for political, economic or military gain). It has recently been a resurgent topic of discussion within government policy and academic circles. Its definition continues to be debated[2] but the pursuits of cyber power range from national cyber resilience, soft power projection through strategic alliances and partnerships, influence and technology exports, to harder power projections such as cyber effects.

The concept of Cyber Power as a lever of power is still evolving, including how a nation grows its own Cyber Power and then realises its enhanced benefits. It tends to be seen as a geopolitical construct, so inviting the concept of global and regional cyber power. Core among definitions of Cyber Power is that it must be considered in the wider context of other instruments of power.

Particular challenges come when situating Cyber Power within the broader definition of power and alongside its traditional instruments such as diplomatic, military and economic – through which capacity a nation can direct or influence the behaviour of others or the course of events.

[1] Such as disruption of adversary systems in order to mitigate a direct threat to the nation

[2] See Harvard Belfer Centre National Cyber Power Index, the IISS Cyber Power Net Assessment and the UK National Cyber Strategy for definitions.



What is the Cyber Domain?

As an overarching term, cyberspace is often interchangeable with the broader concept of the digital operating domain – in which hardware, software and information assets sit. This is illustrated by one aspect of Cyber Power, which is the security of a nation's digital economy, making a nation an attractive prospect for digital trade and Foreign Direct Investment. In the military context, nations such as the UK see cyber as an operational domain or battlespace to be considered alongside the domains of Land, Sea, Air and Space. Across multiple contexts, cyberspace touches all aspects of modern life and as such all aspects of government operations and civilian life.

Focus on the military

This paper explores the context of Cyber Power and its implications for a nation's military. In this context, Cyber Power must sit alongside the concepts of naval, air and land power. Similarly, the pursuit of objectives within cyberspace as an operational domain must sit alongside the traditional operating domains of Land, Sea and Air. Multi-domain operation is important in pulling information and coordinating actions across all operational domains (including cyberspace) and reaps the benefit from any augmentation in cyber capabilities that can be used in concert with other levers of power.

In the military context, nations such as the UK see cyber as an operational domain or battlespace to be considered alongside the domains of Land, Sea, Air and Space. Across multiple contexts, cyberspace touches all aspects of modern life and as such all aspects of government operations and civilian life.

Military power

At a national level, power is asserted via different organisations within (and beyond) its government. For example, a nation's ministry of foreign affairs has a leading role in building and leveraging diplomatic influence. By contrast, a nation's military is the organisation that is charged with defence of the nation in the physical domain – i.e. protection of territorial sovereignty and safety from other nation's militaries (among other remits that vary between countries). Within this core mandate, the military is empowered to undertake offensive action on behalf of the nation against adversaries, whether enacted via a declaration of war or as a defensive posture. As such, military power represents an overt threat to foreign nations, which is intended to deter hostility and interference, as well as actively defend and compel those nations.

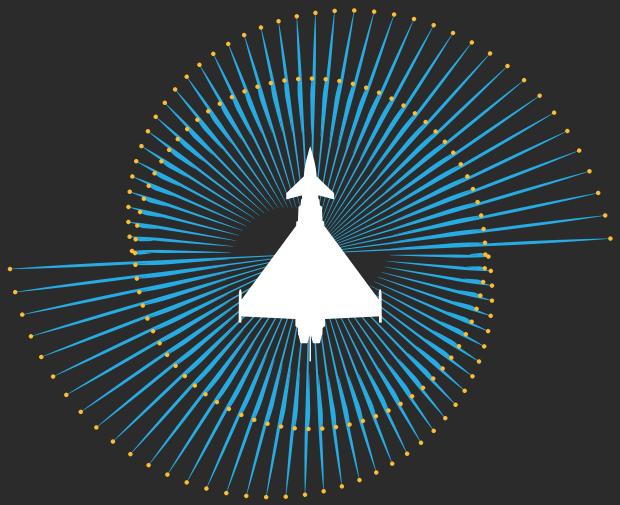
Military power, and the deterrence in behaviour, is influenced by the actions and perceptions of others, as well as by its own capabilities and actions. Clearly, the overt capability of the military is measured and tested through actual warfighting. Many nations are rarely at war, but maintain their military as a fighting force in peacetime, as a standing deterrent. As a result, this deterrent nature of the military is fundamentally the perception by governments of foreign nations (and its citizens) that another nation's military is a force of equal or superior power to their own. This perception is influenced by the historical ability to successfully deploy this capability in times of war, or outside wartime through tests and exercise. Notwithstanding such demonstrations, the active efforts to influence or manipulate the perceptions of other nations is a growing space, both above the threshold of war and below it.

Information warfare and CEMA

A modern military may operate in the Air, Sea, Land or even Space domains, but all these geographically bounded domains intersect with the Cyber domain. The Cyber domain is often the most accessible aspect of any nation's assets (including its military's assets). As subthreshold competition continuously drives forward the evolution of military operations, via enterprise networks, digitalisation of weapons, and pervasive communications, military assets become ever more accessible via the cyber domain. Increasingly, military defensive operations include cyber and electromagnetic effects and activities (CEMA) to disrupt or destroy adversary assets or to acquire information from them.

Along with Information Warfare, CEMA is increasingly pervasive in subthreshold activity. The ambition underpinning subthreshold competition is to undermine another nation's military capability without ever exceeding the threshold for conflict. Cyber capabilities may be leveraged in overt acts of aggression and covert acts of national disruption, and if fear is the primary foundation for a military's contribution to a nation's power in peacetime, then doubt tilts the balance of power to the favour of other nations. The Cyber domain is one of the most effective environments for Information Warfare. Cyber Power is thus more than just a technical race to superiority, it is the ability to withstand Information Operations enacted through the cyber domain.

The next section discusses how a nation's armed forces has responsibilities across all of the aspects that make up Cyber Power.



The Cyber domain is often the most accessible aspect of any nation's assets (including its military's assets).

2 How a military contributes to Cyber Power

Offensive cyber and CEMA

A military has a contributory element to many aspects of Cyber Power. Typically the first assumption about Cyber Power in a military context is that it implies growing offensive capabilities. As an agent of force against another nation or hostile aggressor, the military may deploy effects in the Cyber domain against adversary digital assets in theatre, as an alternative to overt firepower to achieve its. Objectives have not broadly changed, however the means of achieving them have evolved. Examples such as disrupting or destroying communications platforms and other technical systems may be achieved with cyber effects as an alternative option to kinetic effects. The intelligence functions of the Armed Forces may also undertake interference of computers and phones for the purposes of information gathering or monitoring of adversary activity for future benefit, and may use cyber effects to achieve those objectives. CEMA effects offer a set of options for military objectives, and Cyber Power implies the effective use of the Cyber domain towards this end.

CEMA capabilities are harder to build and wield effectively, hence there's a whole capability development and operating model that's newer and less well defined.

In some nations, the role for offensive cyber sits with the Intelligence and Security Services. However in many nations the military has partial or complete responsibility for national capability for strategic offensive cyber. Examples include the UK where the National Cyber Force is a partnership between the military and the intelligence community; the US where both the NSA (with their Title 50 role directing it towards an intelligence function) and USCYBERCOM (with their Title 10 role); and in Australia where the ASD report into the Minister for Defence.

Building on the multitude of other current and emerging cyber and electromagnetic effects that exist across a modern military – on the ground, on air platforms and at sea – many militaries are investing heavily in capabilities in this space.

Cybersecurity – securing the mission

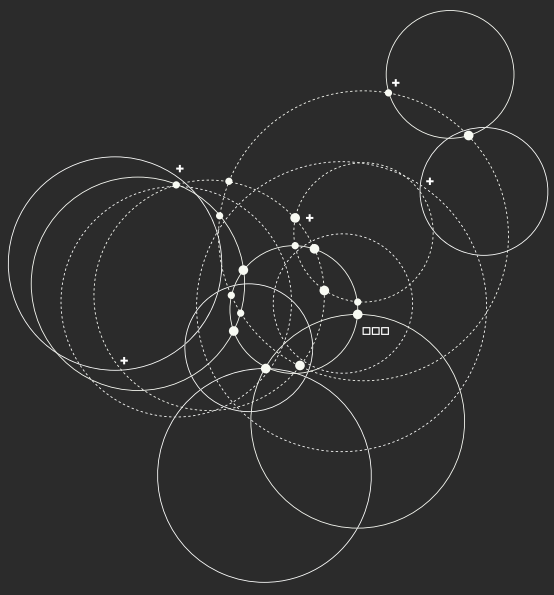
Whilst Cyber Power includes a nation's ability to leverage advanced cyber-related capabilities to enhance its military warfighting ability, the military is of no net benefit to a nation's overall Cyber Power if key adversaries find the military to be a soft target for subversion via cyberspace. A military needs to be able to operate in a contested Cyber and EM environment as it does in a physical environment. This means it needs intelligence, defensive, and optionally offensive capabilities.

Put simply, the ability of a military to engage in cyber warfare is entirely dependent on its ability to defend itself against cyber and electromagnetic attacks. As such, Cyber Power is fundamentally linked to the cyber defence and resilience of the military's own digital assets, and the ability for the military to resist adversary attacks. The military must have a proportionate capacity to harden and defend its own Information and Operational Technology systems across its global footprint – deployed and at home – and be able to continue operations in a secure manner in hostile environments, whether on land, at sea or in space. Furthermore, the operational security needs of a military's activities must be considered, for example resilient access to secure communications infrastructure. It must be a difficult target for adversaries in all areas of operation in a variety of dynamic operational contexts.

Responsibility for securing the military enterprise, deployed missions and platforms against cyber attack does not only sit with the military. Whilst a military has to secure its enterprise, which includes securing its deployed missions and platforms, some of this responsibility must be devolved to periphery organisations outside the core of the military, including both the immediate and the extended supply chain. Outsourcing is approached differently in different countries, and whilst it is clear that it cannot be the military's role to harden an entire nation, the extended supply chain is often the softest target and thus the weakest link. Industry partners, both sovereign and global, therefore fall within this aspect of cyber defence, and by extension their effectiveness in contributing to the overall security of the military mission contributes to the nation's Cyber Power.

Technology advantage

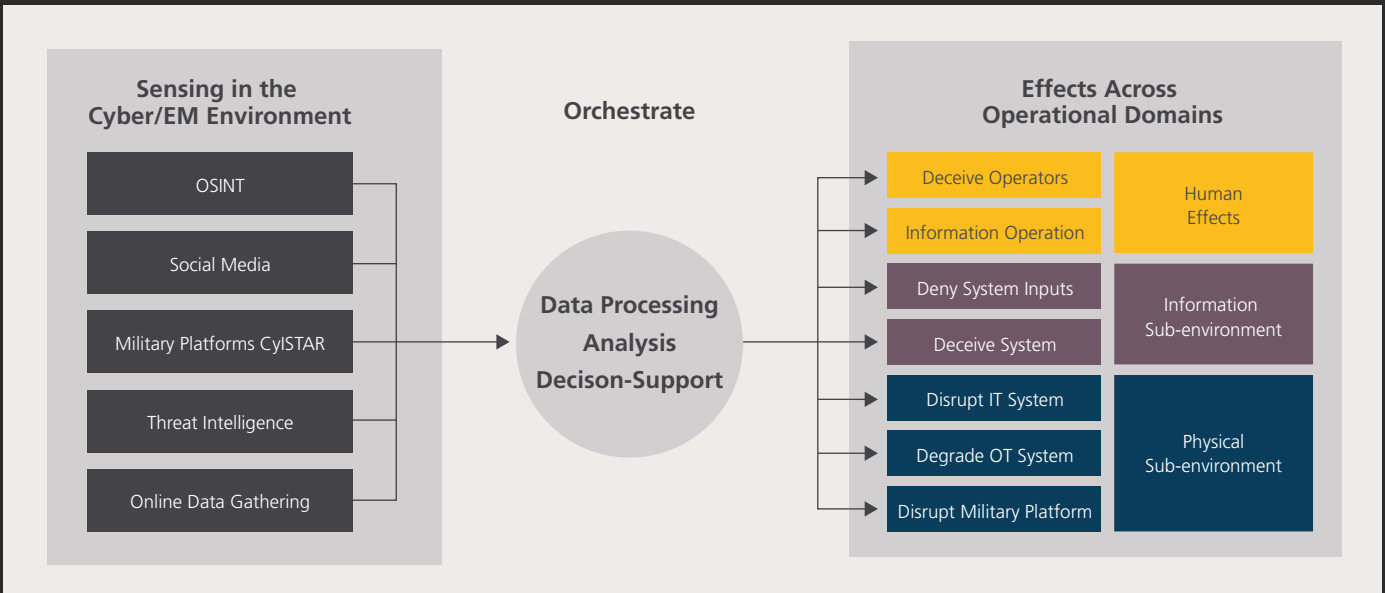
Furthermore, the military also embodies a significant degree of science and technology, especially in the field of the research and development that contributes to its effectiveness in cyber warfare. The presentation of mature and sophisticated cyber capabilities and defence in the deployed mission (illustrated by the Carrier Strike Group) is a contribution to military cyber power in the same way as kinetic and physical attributes attest to military power. Again, this advantage is drawn from an extended ecosystem beyond the core military - the capabilities are presented by the military but it is drawn from combined activities with the intelligence community, from research establishments and from the depth and breadth of the industrial base. In more ways than one, industry contributes to the military cyber power and the ability of the military to stimulate and exploit cyber capabilities from its industrial base attests to a nation's cyber power. Similarly, interoperability and joint capabilities with international partners attests to the extension of cyber power through alliances.



The military is of no net benefit to a nation's overall Cyber Power if key adversaries find the military to be a soft target for subversion via cyberspace.

Integration of capabilities

The concept of multi-domain integration (MDI) describes how military operations across all domains are fully integrated to achieve a smarter, amplified force. A fully integrated military is an effective force both above and below the threshold. The cumulative effect of digital resilience, world leading science and technology research, and evolving offensive capabilities creates a strong cyber capability. MDI integrates aspects of the broader nation's defensive posture that are reflective of its national cyber defence capabilities. It also builds and leverages defensive situational awareness that inform the military and wider national response, by pulling inputs from sensors across all five domains, to enable decisions and actions across all five domains, as shown in the diagram below . These actions may of course be both defensive responses and offensive cyber responses or via kinetic or diplomatic means.



Where conflict is above the threshold of war, Cyber Power will be enhanced where the military is able to leverage (in isolation or as part of an allied community) advanced offensive cyber and offensive electromagnetic effects against an adversary.

However there is persistent sub-threshold competition at play between nations that exists outside a traditional definition of war and pervades all five operational domains. Some activities are highly effective when carried out below the threshold, including restricting adversaries' freedom of movement whist enabling one's own, and preparatory reconnaissance and interference activities that lay enabling foundations for quick responses in the future when conflict does eventually escalate.

Information Advantage continues to be relevant to the role of the military and this has significant elements that exist in this subthreshold space. The Russian approach[3] of a parallel technical and psychological actions reflects on the high priority that Cyber Power plays in the state's approach to conflict and how the narrative is controlled during that conflict.

[3] Impacts of Russian Information Operations: Technical and Psychological Aims - ICDS

Perception and will

At a human level, a soldier's will is essential if that soldier is to be the best asset possible. If cyber related effects can be used to undermine the human element of an adversary's forces – by whatever means (and there are many) – then this is likely a far less costly option to weaken the adversary than alternate options available.

Furthermore, if the overall perception of a military is its most significant day-to-day contribution (outside times of war) to a nation's overall Power projection, then strategic and persistent degradation of that perception in the mind of soldiers, military leadership, government leadership and a nation's citizens is therefore a powerful lever that may diminish the net Power of a nation. Essentially every offensive action points to a defensive need.

Integration into national and international Cyber Power

All the activities discussed thus far are references to how a military force delivers hard power. MDI doctrine reminds us that military operations are part of (not in isolation to) wider government and deliver national objectives.

It should not be forgotten however that soft power – influence through diplomacy for example – is also enhanced through the nation's military, and that elements of this are contributory to net Cyber Power. Military support this effort directly and indirectly, through training, outreach, joint exercises and capacity building, and disaster relief. Must of this is applicable and very relevant in cyberspace such as cyber capacity building, joint cyber exercises and collaboration on cyber incidents.

Governments maintain a global network of relationships through diplomatic missions that include military postings (such as defence attaches). A clear example is that through such discourse opportunities for technology influence and opportunities for new operational alliances may emerge.

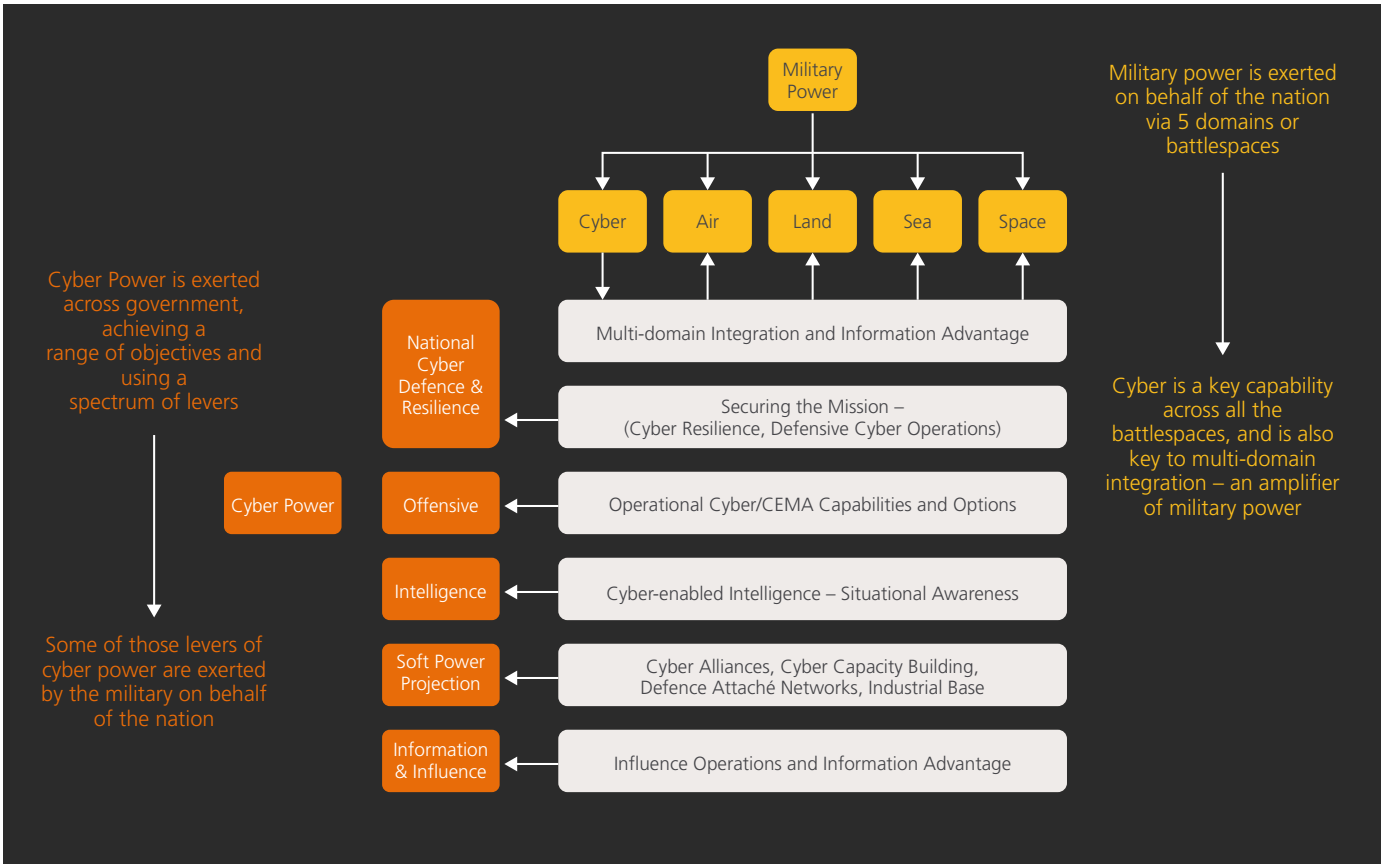
It is through these relationships that a nation is able to promote behaviours that align to its own policies and beliefs, build capacity in its partners, and deter practices that directly or indirectly pose a future threat.

As an emerging capability in many countries around the world, the creation of strong alliances enable collective action against shared threats and collaborative activities that prevent degradation of one nations security posture through conflict with less able allied nations. Alliances are always a strong component of power, and military collaboration on cyber capabilities is another opportunity for building such alliances – which could enable joint exercising, joint operations or sharing of training infrastructure amongst other things.

As an emerging capability in many countries around the world, the creation of strong alliances enable collective action against shared threats and collaborative activities that prevent degradation of one nations security posture through conflict with less able allied nations.

3 Conclusion

In conclusion, while it is evident that the military is a significant component to a nation's Cyber Power as it is with the traditional instruments of power, its actual net contribution to Cyber Power depends on securing its missions, maintaining operational resilience, and leveraging its industrial base and partnerships at the increasing pace of warfare and subthreshold operations. The intersection that exists between traditional military power and cyber power is complex, as shown by the graphic below .



The avenues created by global digitisation for arms-length effects that are exploitable by competent cyber actors will continue to transform the landscape of power. But this applies equally to allies as it does to adversaries, and thus the capability to project effects needs to be equalled or exceeded by the ability to resist them.

The digital footprint of a military goes beyond the boundaries of the military enterprise, enveloping a vast supply chain of industry partners, as well as other government departments and academia and importantly, allies. This must be considered in any consideration of cyber resilience of the military. But while this ecosystem can present risks, it can also serve to bolster and evolve the sophisticated cyber capabilities of the military.

Not all the elements are in the military's control. Sophisticated and persistent Information Warfare targeted at destabilising a nation's military and influencing the future direction (strategy, budget or movement) can have as damaging outcomes as kinetic warfare, partly because they are harder to detect and protect against. The development of national resilience to such activities – noting they may have equal or greater detrimental impacts across the whole nation and its society – must be as much a cornerstone of the resilience to adversary capabilities as resistance to other more direct sub-threshold (and above-threshold) cyber effects.

For a military to be a net contributor to a nation's projection of Cyber Power in today's digital environment, it must be able to operate in the contested Cyber/EM space in any area of operation, primarily through the continued evolution of defences and of operational resilience that keeps pace with change. If it chooses to develop offensive CEMA capabilities for purposes of attack or defence, it must develop its operating model and capability pipeline such that CEMA is well understood, used to the greatest effect, and not hindered by uncertainty or other barriers. This requires skills and familiarity but also analysis and processes to remove the uncertainty from deployment of CEMA effects.

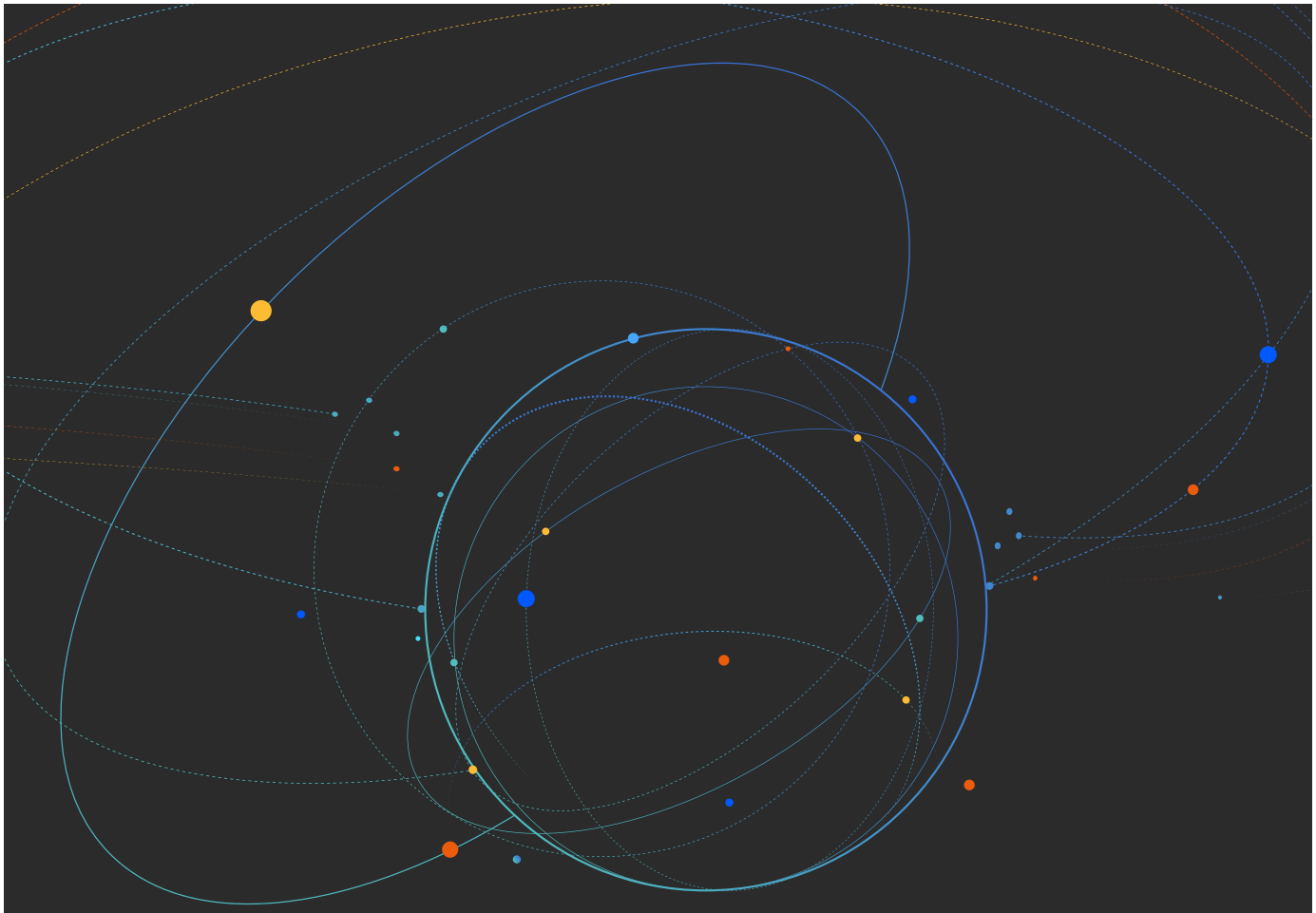
But Defence must do more to support national Cyber Power ambitions than develop CEMA capabilities. Soft power is as important as hard power, and thus an ability to best leverage a nation's global diplomatic equities such as defence attaches is as fundamental as developing sophisticated cyber offensive and defensive capabilities.

Furthermore, in many nations the military also needs to nurture alliances and relationships as part of their export agenda, enhancing others' capabilities in order to increases their own net Cyber Power, and thus must be better aligned with other government departments and allies – both technically and operationally.

This must include demonstrating defensive cyber capabilities in training and synthetic exercises, application of strong governance, and clear recognised linkages to intel and strategic capabilities.

Finally, it is hard to measure and trend the military's contribution without the concept and implications of Cyber Power itself being evolved to be understood and thus measurable in a more consistent manner. These efforts should continue and the military should engage in this debate, which will help militaries confidently map out their responsibilities in the net enhancement of Cyber Power.

The digital footprint of a military goes beyond the boundaries of the military enterprise, enveloping a vast supply chain of industry partners, as well as other government departments and academia and importantly, allies.



About the authors

Miriam Howe

is Lead Cyber Consultant at BAE Systems Digital Intelligence

miriam.howe@baesystems.com

Chris Holt

is a National Cyber Mission Pre-Sales Lead at BAE Systems Digital Intelligence

chris.w.holt@baesystems.com

0 1 1 0 0 1 1 0 1 0 1 0 0 1 1
1 0 1 0 1 0 0 1 1 0 1 0 1 1 1

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
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

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