



Shutterstock: Pasuwan

Sep 20, 2019 22:01 BST

Outsourcing global cyber norms

Making cyberspace safe and secure on a global scale has long been on the agenda for the public and private sectors alike. So far, the responsibility for delivering this has mostly sat with governments, with the expectation being that organisations will comply with regulations that have been put in place by the state.

However, it often doesn't get this far. The diverging interests and behaviours of governments can make it difficult for them to come to an agreement on what cross-border cyber norms – namely the behaviours, processes and regulations that make the internet and cyberspace safe and secure – should look like.

When governments do come to an agreement, it is often lacking in detail. This leaves room for interpretation, which can make establishing global cyber norms difficult, and make any agreement on how to implement them in practice impossible.

This is the case with current attempts by the United Nations (UN) to come to an agreement on what is and isn't acceptable in cyberspace.

Current consensus on international attempts to establish cyber norms includes a high-level agreement that governments should 'commit to sharing information and working in partnership' and 'implement coordinated vulnerability disclosure mechanisms'. While the principles are important, there must also be a shared interpretation and specific, defined actions if individual nation states are to put these into practice.

How can the private sector help?

Turning this traditional model on its head could be part of the answer when it comes to establishing international cyber norms.

This is where the corporate world can step in. There are a number of commercial incentives for the private sector to begin to lead the conversation around cyber norms – from securing their own technology and systems, to boosting their reputation and removing the need to comply with multiple regimes across the world.

If organisations begin to work together to change behaviours and actions in cyberspace, without being mandated to do so, then the state and governments can understand what does and doesn't work, and have the option to formalise this behaviour. This would then help lead to internationally agreed and acted upon cyber norms, rules, and regulations.

We have already started to see this in action through initiatives such as the Cybersecurity Tech Accord and the Charter of Trust. Both of these initiatives, announced in 2018, have been led by the private sector and emphasise broader industry involvement and ownership when it comes to defining objectives and actions. Crucially, both have delivered tangible results, including the adoption of vulnerability disclosure policies across the industry and driving cyber security requirements across the supply chain.

The establishment of a global set of cyber norms is undoubtedly complex, and the journey towards this is likely to be bumpy.

However, while corporate initiatives such as the Cybersecurity Tech Accord are still in their early stages, they have already shown significant progress. To ensure that these initiatives continue to evolve and succeed, it's important that processes are put in place to ensure that the private sector has a seat at the table when decisions are made.

To bring more private businesses into the fold, incentives should be introduced to ensure that the corporate action and purpose private businesses align with efforts to create a global set of standards. Ultimately, establishing and maintaining collaboration between the private and public sectors could be a key step towards a truly open, secure, peaceful and accessible cyberspace.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts



NCC Group Press Office

Press Contact

All media enquires relating to NCC Group plc

press@nccgroup.com

+44 7824 412 405

+44 7976 234 970



NCC Group - Financial Media Enquiries

Press Contact

Maitland AMO

Financial Results Media Enquiries

+44 (0)20 7379 5151



Regional Press Office - North America

Press Contact

NCCGroup@cdc.agency

+1 408 776 1400

+1 408 893 8750