From the cyber proliferation threat all the way to Pall Mall

The first dedicated conference on this topic – and an insight into the NCSC assessment work behind it.

Annabel W

Earlier this month the UK and France hosted the first, dedicated conference on tackling the threat from commercial cyber proliferation.

It brought together a wide range of organisations and views – states, tech companies, civil society representatives, academia, cyber security, investors, researchers and private industry – to define the issue, and explore how we can work all together on this issue, ultimately to improve global security and society.

The end result was the signing of the Pall Mall Process declaration: a new international initiative to explore policy options and new practices to address this shared threat.

> *In the NCSC, we recognise this is a complicated issue with no quick fixes. It requires action and commitment from the full range of stakeholders, and everyone has a unique part to play. By coming together — under the Pall Mall pillars of accountability, precision, oversight and transparency — we can reduce the impact of irresponsible activity that threatens all of our cyber security.*

Jonanthan Ellison, NCSC Director of National Resilience and Future Technology

Digging deeper into the assessment

The NCSC first published a report about this topic at CYBERUK 2023. Generally, in threat assessment work, we are used to asking two key questions: what is the *intent* and what is the *capability* of an actor? The heart of assessment work is to answer difficult, uncertain questions using all-source information and structured analysis to provide independent judgements on cyber threat to inform decision making.

The impact on cyber threat from commercial cyber proliferation is the epitome of one of those difficult and uncertain questions.

More about those knotty questions

A particular challenge of this topic was to understand *how* you assess intent when the developer, seller, or even investor, in a capability is one or more steps removed from the threat activity and where the capability itself might have legitimate as well as malicious uses?

And on capability, are you assessing how sophisticated a product or service is or how effective it is at doing what the actor needs it to do? Or are you assessing who has access to that capability and their use of it or are you assessing how accessible it is and therefore its potential use at scale?

And the conclusion?

In the end, on this question, the answer the NCSC assessment team reached was: all of the above. More formally, we concluded:

“Increased demand, coupled with a permissive operating environment, will almost certainly result in an expansion of the global commercial cyber intrusion sector, driving an increased threat to a wide range of sectors over the next five years.”

The real-world effect of this will be an expanding range and number of victims to manage, with attacks coming from a more unpredictable range and type of actor.

This is the assessment if there is no change.

Advance to GO

The journey ahead to reduce the impact on security and society of commercial cyber proliferation is long, but coming together and launching #PallMallProcess last week felt like we are finally moving from 'Go' on the board.

Annabel W
Global Issues Team Lead, NCSC Assessment

WRITTEN BY

Annabel W
Global Issues Team Lead,
NCSC Assessment

PUBLISHED

15 February 2024

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector

PART OF BLOG

Inside the NCSC