What makes a responsible cyber actor: introducing the Pall Mall industry consultation on good practice

Calling vulnerability researchers, exploit developers and others in the offensive cyber industry to share their views.

Dave L

The commercial cyber intrusion industry operates in a complex landscape where cutting-edge capabilities can both serve essential security functions and lead to potential misuse. These tools and services, which run the full spectrum from vulnerability research (VR) to access as a service, play a vital role in tackling serious crime and protecting national security. Yet without clear standards and accountability, the same capabilities can enable unacceptable activities and undermine the digital security that underpins our daily lives. These tools need to be developed and used with the right balance of transparency, precision, accountability and oversight.

Why your voice matters

This tension sits at the heart of the Pall Mall Process, an initiative launched by the UK and France in 2024. The Pall Mall Process is an international multistakeholder approach dedicated to **tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs)**. It brings together a wide range of organisations and perspectives – from governments, technology companies, civil society, academia, the cyber security community and investors, to commercial offensive cyber intrusion companies themselves – to define the problem, and explore how we tackle it together.

The National Cyber Security Centre (NCSC) is contributing our technical expertise to help develop a process that supports responsible actors, (the UK's approach to responsible cyber power published on gov.uk) whilst addressing the risks posed by those operating without appropriate safeguards. We, our FCDO

colleagues, and their French counterparts are engaging widely across society, but due to the discreet nature of this market we are seeking additional insights from people working in vulnerability research, exploit development, and the wider offensive cyber industry to get this right.

From state commitments to industry standards

In April 2025, the Pall Mall stakeholders launched a **Code of Practice for States** which sets out the principles of responsible engagement with the cyber intrusion market. To date, the Code of Practice for States has been supported by over 27 countries.

But governments are only half the solution. The real experts in how an industry can be improved are those in the industry itself. The next stage of the Pall Mall Process is to develop a complementary set of guidelines for industry.

What do we mean by commercial cyber intrusion capabilities?

CCICs are tools or services offered by commercial entities to enable advanced cyber operations. They include:

- vulnerability research
- exploit development
- malware creation
- command and control
- hacking as a service
- access as a service

These capabilities may be offered via a business-to-business model – as part of a complex supply chain; or in a business-to-customer model, directly to end

users – most commonly law enforcement or intelligence services internationally.

The market for CCICs encompasses a wide variety of cyber intrusion companies offering products and services that are continually evolving and diversifying. It includes an interconnected ecosystem of researchers, developers, brokers, resellers, investors, corporate entities, operators, and customers, including states. Everyone in this ecosystem has a part to play in encouraging/advocating responsible use of CCICs.

> CCICs are an essential part of many countries' toolkits for tackling serious crime, countering national security threats, and protecting citizens. But without the necessary safeguards, their use can be dangerous and destabilising. The Pall Mall process seeks to maximise the positive use made of CCICs while striving to eradicate their harmful use.

The NCSC's unique role

As the UK's National Technical Authority for Cyber Security, the NCSC benefits from its position within an organisation operating in both offensive and defensive capacities, providing a unique perspective on CCICs. We:

- Run the **UK Equities process**, ensuring responsible handling of discovered vulnerabilities.
- Engage with the VR community through our **Vulnerability Research Initiative (VRI)** function.
- Defend the UK from cyber threats.
- As NCSC Assessment, provide independent, all-source intelligence assessments to UK government customers on the threat actors, including CCICs.
- Are part of GCHQ, the UK's signals intelligence agency who, governed by strict legislation, conduct computer network operations.

In essence, our role is to:

- provide expert advice to inform policy makers on the balance of risks and benefits of CCICs
- drive our collective engagement to ensure the CCIC market operates with the **right balance of transparency, precision, accountability and oversight to enable us all to protect our digital world and defend against threats**.

Why we need guidelines for industry

This is about bringing an industry (that has often worked in the shadows) into the open – creating transparency and accountability. It's also about making sure that the next generation of technical talent knows the full spectrum of cyber career paths available to them, both defensive and offensive.

To improve our collective security, human rights, digital trust and the industry itself, we would like industry guidelines that:

- agrees what responsible activity in this marketplace looks like
- enables the community to respond collectively to tackle the irresponsible use of CCICs

---

We want to hear from you

As the Pall Mall Process moves into its next phase focusing on **industry guidelines**, we want to:

- Hear from the people building and selling offensive cyber capabilities to understand the market forces and drivers, capturing their motivations and getting their thoughts on how the industry can operate going forward.
- Help shape the market so that responsible participants can flourish, while making life harder for irresponsible actors.

So, if you work in this field and would like to contribute, please get in touch with the FCDO.

Dave L
Technical Director for Cyber Marketplace

WRITTEN BY

Dave L
Technical Director for Cyber Marketplace

PUBLISHED

2 December 2025

WRITTEN FOR

Cyber security professionals

PART OF BLOG

Events and initiatives