NCSC warns of enduring and significant threat to UK's critical infrastructure

The NCSC's seventh Annual Review raises awareness of the increasingly unpredictable threat landscape.

- National Cyber Security Centre – part of GCHQ – uses Annual Review to raise awareness of increasingly unpredictable threat landscape.
- UK's critical sectors facing 'enduring and significant' threat, in part due to a rise of state-aligned groups and an increase in aggressive cyber activity.
- Review calls for continued collaboration with allies and industry in countering epoch-defining challenge posed by China.
- Rise of artificial intelligence and evolving geopolitical landscape highlighted as significant areas of risk to UK electoral processes.

The UK's cyber chief has today signalled that the threat to the nation's most critical infrastructure is 'enduring and significant', amid a rise of state-aligned groups, an increase in aggressive cyber activity, and ongoing geopolitical challenges.

In its latest Annual Review, published today, the National Cyber Security Centre (NCSC) – which is a part of GCHQ – warned that the UK needs to accelerate work to keep pace with the changing threat, particularly in relation to enhancing cyber resilience in the nation's most critical sectors.

These sectors include those that provide the country with safe drinking water, electricity, communications, its transport and financial networks, and internet connectivity.

Over the past 12 months, the NCSC has observed the emergence of a new class of cyber adversary in the form of state-aligned actors, who are often sympathetic to Russia's further invasion of Ukraine and are ideologically, rather than financially, motivated.

In May this year, the NCSC issued a joint advisory revealing details of 'Snake' malware, which has been a core component in Russian espionage operations carried out by Russia's Federal Security Service (FSB) for nearly two decades.

Today, the NCSC is reiterating its warning of an enduring and significant threat posed by states and state-aligned groups to the national assets that the UK relies on for the everyday functioning of society.

More broadly, the UK government remains steadfast in its commitment to safeguarding democratic processes. Recent milestones include the implementation of digital imprint rules under the Elections Act to foster transparency in digital campaigning, fortifying defences against foreign interference through the National Security Act, and advancing online safety measures through the implementation of the Online Safety Act.
NCSC CEO Lindy Cameron said:

> "The last year has seen a significant evolution in the cyber threat to the UK – not least because of Russia's ongoing invasion of Ukraine but also from the availability and capability of emerging tech.
>
> "As our Annual Review shows, the NCSC and our partners have supported government, the public and private sector, citizens, and organisations of all sizes across the UK to raise awareness of the cyber threats and improve our collective resilience.
>
> "Beyond the present challenges, we are very aware of the threats on the horizon, including rapid advancements in tech and the growing market for cyber capabilities. We are committed to facing those head on and keeping the UK at the forefront of cyber security."

Defending Democracy

The Annual Review highlights a new trend of malicious actors targeting the personal email accounts of high-profile and influential individuals involved in politics. Rather than a mass campaign against the public, the NCSC warns that

there is a “persistent effort” by attackers to specifically target people who they think hold information of interest.

The NCSC assesses that personal as opposed to corporate accounts are being targeted as security is less likely to be managed in depth by a dedicated team. In response, earlier this year the NCSC launched a new opt-in service for high-risk individuals to be alerted if malicious activity on personal devices or accounts is detected and to swiftly advise them on steps to take to protect themselves.

The Annual Review also highlights how the next general election will be the first to take place against the backdrop of significant advances in artificial Intelligence (AI), which will enable and enhance existing challenges.

More specifically, the NCSC assesses that large language models (LLMs) will almost certainly be used to generate fabricated content; that hyper-realistic bots will make the spread of disinformation easier; and that deepfake campaigns are likely to become more advanced in the run up to the next nationwide vote, scheduled to take place by January 2025.

The NCSC also assesses that democratic event, such as elections, almost certainly represent attractive targets for malicious actors and so organisations and individuals need to be prepared for threats, old and new.

In response, the Annual Review highlights the work of the NCSC and wider government in weaving resilience into the fabric of the UK’s democratic processes ahead of the next election, which includes the establishment of the Joint Election Security Preparedness (JESP) unit.

China

As part of broader risks to the UK’s cyber security, the Annual Review highlights that the NCSC continues to see evidence of China state-affiliated cyber actors deploying sophisticated capability to pursue strategic objectives which threaten the security and stability of UK interests.

In May, the NCSC and international partner agencies issued a joint advisory highlighting how recent China state-sponsored activity had targeted critical infrastructure networks in the US and could be applied worldwide.

In response to the ongoing challenge from China, the NCSC has called for continued collaboration with allies and industry to further develop its understanding of the cyber capabilities threatening the UK.

Russia

The Annual Review highlights how Russia continues to be one of the most prolific actors in cyberspace, dedicating substantial resources towards conducting operations around the globe and continuing to pose a significant threat to the UK.

The NCSC has continued to observe cyber activity targeting Ukraine by Russia and Russia aligned actors, though these appear to by opportunistic rather than strategic. Overall, the impact on Ukraine has been less than many expected, in part due to well-developed Ukrainian cyber security and support from industry and international partners, which includes the UK's own cyber programme.

Elsewhere, Russian language criminals operating ransomware and 'ransomware as a service' models continue to be responsible for the most high-profile cyber attacks against the UK.

The ransomware model continues to evolve, with a sophisticated business model, facilitating the proliferation of capabilities through the 'ransomware as a service' model. This is lowering the barriers to entry and smaller criminal groups are adopting ransomware and extortion tactics which are making a huge impact.

Iran

While less sophisticated than Russia and China, Iran continues to use digital intrusions to achieve their objectives, including through theft and sabotage.

In September 2022, the NCSC and international partners issued a cyber advisory highlighting that actors affiliated with Iran's Islamic Revolutionary Guard Corps (IRFC) targeted known vulnerabilities to launch ransomware operations against multiple sectors, including critical national infrastructure organisations.

In January 2023, the NCSC warned of the threat from targeted spear-phishing campaigns and against UK organisations and individuals carried out by cyber actors based in Iran. Spear-phishing involves an attacker sending malicious links, for example via email, to specific targets to try to induce them to share sensitive information.
The attacks were not aimed at the public but targets in specified sectors, including academia, defence, government organisations, NGOs, think-tanks, as well as politicians, journalists, and activists.

NCSC Annual Review 2023

Looking back at the National Cyber Security Centre's seventh year and its key developments and highlights, between 1 September 2022 and 31 August 2023.

View the Annual Review

PUBLISHED

14 November 2023

WRITTEN FOR

Public sector

Cyber security professionals

Large organisations

NEWS TYPE

General news