
Nigel Inkster Charlotte Kelloway December 2nd, 2025

# How much should the UK worry about cyberattacks?

*Cyberattacks are increasingly being used as a part of warfare, and states, as well as private companies, are increasingly having to invest in cybersecurity. In this interview,* ***Charlotte Kelloway*** *asks* ***Nigel Inkster*** *about the extent to which we should worry about the ability of cyberattacks to seriously damage the UK.*

---



---

***What is the difference between a cyber-attack and cyber war?***

A cyber-attack speaks for itself: It is a hostile intrusion into a network for whatever purpose, sabotage, espionage, criminality, ransomware, that kind of thing.

Cyber warfare is a difficult and I think contested term. I don't think anybody really knows what it means. And to talk about cyber warfare as something that implies that it is separate and discreet from any other form of warfare, I think is highly misleading.

If we look at real world examples, for example, what's happening in Ukraine, we see cyber operations being undertaken by both sides all the time as a subset of other belligerent activities. And I think that is probably the most useful way of looking at the distinction.

I think some years back, and certainly in the early days of the internet, there was this sense by many thinkers and strategists that cyber warfare conceived of basically as activities designed to digitally disable an opponent, could in and of itself be decisive.

We've been through this throughout history. There's been a succession of examples where strategic thinkers have identified a particular capability as likely to prove quick and decisive. During the 1930s, it was aerial bombing. The bomber always gets through, always delivers. People like Giulio Douhet, Billy Mitchell, Arthur Harris argued that the bomber would be a decisive capability that would quickly bring an opponent to the negotiating table. And, of course, that proved not to be the case and we've seen it with a number of other capabilities. I think cyber has just been the latest in this series of so-called killer-app capabilities that quickly and decisively end a conflict, but such things just don't exist.

***How prepared would you say the UK was against a major cyber-attack on our critical infrastructure?***

I think if you were to ask the National Cyber Security Centre, they would say that we're not doing badly, but nowhere near as well as we should ideally be. I think the National Cyber Security Centre has been a significant force multiplier in terms of ensuring UK ability to deal with these attacks. But, of course, they can't be everywhere, they can't be doing everything and they are critically reliant upon government departments, private sector to do the things that they need to be doing in order to minimize the attack surface.

And this is still not happening to anything like an acceptable degree. There are still too many entities out there using legacy systems that are no longer properly protected, that aren't still undertaking on a routine and regular prioritized basis, fundamental cyber hygiene. That has been proven time and time again to offer a high degree of protection against attack.

> *I think there is a growing realization that cyber security is fundamental to the functioning of the state, to the functioning*

*of the private sector, but it's still very uneven.*



We do also have considerable strengths, though. We have GCHQ, which is a formidable operator in and of itself, and also as part of The Five Eyes, Anglo-Saxon Intelligence Alliance. The National Cyber Security Centre has got a lot of buy-in from the private sector. I think at any given point, there are probably about 200 representatives of the private sector working in NCSC and the companies are paying for them to be there, which is a good thing. I think there is a growing realization that cyber security is fundamental to the functioning of the state, to the functioning of the private sector, but it's still very uneven.

***Do we know where the majority of the attacks on the UK are coming from and what form they are taking?***

I find it difficult to answer that question because I'm not on the inside and haven't been for an awful long time. If you were to ask NCSC, I think they would tell you that by far the bulk of their time is spent dealing with ransomware attacks. Criminality, whether it's state-sponsored, state-condoned or just pure criminality.

State-sponsored attacks are taking place all the time, in particular from China, still focusing on things like the theft of intellectual property where the UK still has quite a lot to offer, but also in all the areas. We see the Chinese state attacking a variety of British institutions, universities, think tanks, and any entity that is involved in policy work that impinges, however tangentially, on China's interests is likely to find itself the subject of these attacks.

And then we have Russia, looking opportunistically to inflict damage and to undermine social cohesion and social stability in whatever ways it can. I think those are probably the main players, but we shouldn't underestimate the extent to which ordinary criminality is the source of a major disruption. Online fraud is taking up or should be taking up more police time than other forms of criminality. But the police still, I think, are quite far behind in terms of their capability to deal with these forms of crime. But the fact is a lot more of this is happening online than in the real world and it is a significant challenge.

***We see lots of scary headlines in the news about major cyber attacks on countries like the UK and the US where our national grids will be shut down or internet will be switched off. How realistic do you think these headlines are?***

Well, I think they have to be taken seriously, but we also need to bear in mind that the majority of cyber attacks are temporary and reversible. Once they've happened, you can over time and sometimes pretty quickly work out what's been done and take steps to reverse the impact. If we look at what's happened in Ukraine, for example, in the run-up to the Russian invasion, we saw

Ukraine coming under constant cyber bombardment from Russia. But the Ukrainians were able to leverage assistance from major Western powers and some major western companies like Amazon, like Microsoft, and were able to rapidly recover from some of these attacks. They're still going on all the time, but self-evidently, Ukraine has not been brought to a standstill by cyber attacks.

> *In the run-up to the Russian invasion, we saw Ukraine coming under constant cyber bombardment from Russia.*

And the other thing about cyber-attacks we have to bear in mind is that some of these will take months, years even, to prepare. You need to gather all kinds of intelligence, reconnaissance on the networks before you are able to determine what is going to be an effective form of attack. And these of course are getting more sophisticated and complex all the time.

The point is once you've fired the weapon, you may not be able to use it again. So there's a lot of capability and a lot of effort has been put into using something that may only be deployed once or twice. And having said that, of course, it remains the case that the architecture of the internet is such that, without a fundamental re-architecting of the infrastructure, there are always going to be vulnerabilities that can be exploited.

We're in a kind of constant battle here. Artificial intelligence is also starting to play a factor insofar as AI can potentially identify vectors of attack that had not been previously identified, but at the same time may also play a significant role in developing more effective defensive capabilities.

We are just going to have to see the sort of constant evolution, constant dynamic of attack – defense – counterattack. But in and of itself, I do not believe that a major nation state can be brought to its knees and to the negotiating table just by cyber-attacks.

---



---



*Image credit:* vectorfusionart *on* *Shutterstock*

## About the author

**Nigel Inkster**

Nigel Inkster is Senior Advisor to the International Institute for Strategic Studies (IISS) and Director for Geopolitics and Intelligence at Enodo Economics. In IISS he worked first as Director for Transnational Threats and Political Risk then as Director for Cyber Security and Future Conflict. In the latter capacity he was involved in para-diplomatic dialogues on cybersecurity and military cyber stability with China and Russia. He also served from 2017 to 2019 as a Commissioner on the Global Commission on the Stability of Cyberspace. Prior to joining IISS he served for thirty-one years in the British Secret Intelligence Service. From 2004 to 2006 he was Assistant Chief and Director for Operations and Intelligence.

**Charlotte Kelloway**

Charlotte Kelloway is Media Relations Manager in the LSE Media Relations team and a Producer/ Host for the LSE iQ podcast.

**Posted In:** Foreign Policy and Defence