Lauren Sukin Charlotte Kelloway December 4th, 2025

Lauren Sukin: “The story of warfare throughout history is really a story of technology”

In an interview with Charlotte Kelloway, ***Lauren Sukin*** *discusses what modern cyber warfare looks like, its impact on the Russia-Ukraine war and how cyber capabilities are changing the balance of power on the global stage.*

What is cyber warfare and what does it look like?

When we talk about cyber warfare, we’re really talking about conflict that occurs in the grey zone – an area of competition between states that’s below the threshold of conventional kinetic armed conflict.

Most of the cyber conflict that we see in the world today is relatively limited. It looks like ransomware or phishing, the kinds of cybersecurity incidents that you might be familiar with and even see in your day-to-day life.

But in military strategy, we’re increasingly concerned about how states can use these techniques to affect larger infrastructure, either as a complement to traditional means of warfare or as a potential entry point to disable an adversary’s capabilities and make a future war easier to fight.

We see lots of pre-positioning today where countries like the United States, Russia and China have identified exploits in key infrastructure that their adversaries have, so that if conflict were to break out, we might expect that they could use these cyber tools to try to impair everything from electrical grids and dams to military command and control infrastructure.

How has technology changed warfare throughout history?

The story of warfare throughout history is really a story of technology. In the beginning, there was the evolution from bows and arrows to the building of trebuchets, or improvements in walls, defensive ditches and moats. These technologies determined who had the advantage in warfare, the attacker or the defender.

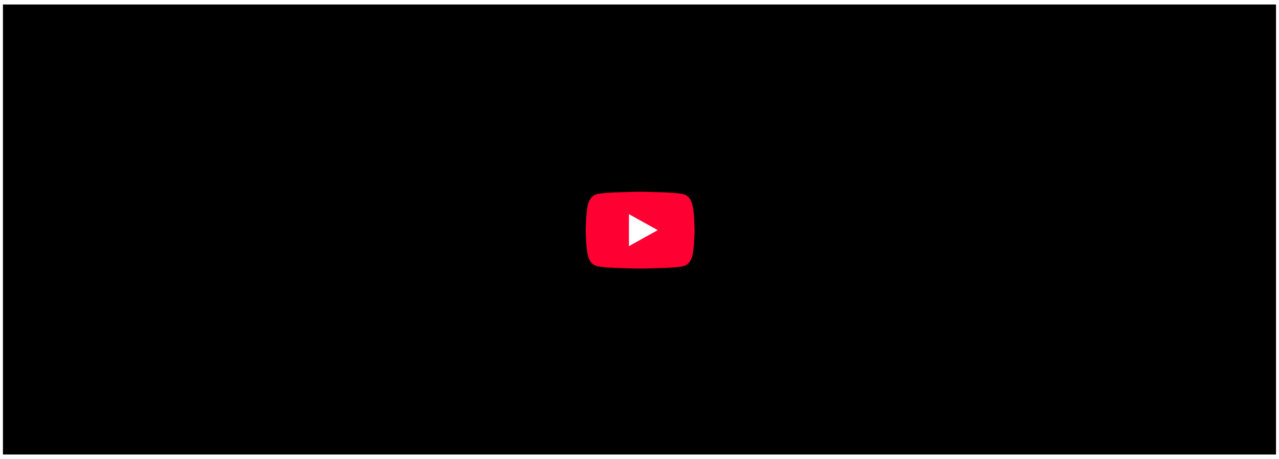
Throughout history, we see this evolution from more basic tools of warfare to technology that's more complicated and for the most part more lethal. When we start to get into the modern era, we have new weapons like nuclear weapons, chemical weapons and biological weapons that are much more advanced than earlier tools of warfare.

And we also have new software capabilities that allow militaries to collect information and communicate with each other. That technology makes us better at fighting wars, but it also introduces new risks into conflict. This is really what we're worried about today, namely how existing and emerging technologies can be integrated with other types of conventional forces and the new risks that come from that.

What is the role of private actors in cyber warfare?

A relatively unique feature of cyber warfare is that it's not monopolised as much by governments. This means there are many private actors, from corporations to non-state hacker groups, that participate in the information warfare space and in the cyber domain.

One way that we see this become important is that states can try to offload responsibility for offensive cyber operations onto hacker groups or other organisations operating within their territory. For example, Russia has repeatedly used these organisations to try to diffuse some of the responsibility for the more offensive techniques that they're using.



There are lots of states that cooperate with or sponsor non-state actor groups like insurgents, but the prevalence of these hacker organisations as private actors connected to governments is particularly present in the cyber domain. We also see private actors play a role in the setup of infrastructure.

If we think about the use of Elon Musk's satellite technology in Ukraine, we're really talking about a single private actor with a unique technology that's able to change the battlefield space in a way that is quite unusual and affects a domain that has typically been dominated by state decision-making.

What has been the role of cyber warfare in the Russia-Ukraine war?

During the Russia-Ukraine war, there's been a lot of speculation about how much Russia might use its relatively advanced portfolio of cyber warfare capabilities to gain the upper hand.

There have been persistent attacks on Ukrainian forces and some hacks that have spilled over and affected allies and even global tech companies. Russia has for the most part maintained much of the infrastructure that allows connectivity in Ukraine for essentially its own purposes. Russia needs to be able to communicate with its own forces and so there's a limit to how much Russia can interfere with the cyber domain.

We've seen a mix of tactics that seem to be designed to slowly degrade Ukrainian forces and antagonise Ukraine's supporters. We've also seen Russia engage in the information space throughout the war, whether that's trying to communicate narratives to Russian civilians and supporters about Russia's success or its reasons for the invasion, or spreading misinformation among Russia's adversaries to try to reduce support for Ukraine.

This has become an increasingly important centre of competition between Russia and Ukraine's western allies. Russia's dominance in the information warfare space raises questions about the ability of alliances to stand together and withstand these types of attacks. The good news is that the western allies continue to invest in their information capabilities and continue to develop techniques for both responding to misinformation and spreading correct information about the conflict.

How has Ukraine used cyber warfare?

One of the things that is important to think about when we talk about the cyber domain is that these are asymmetric capabilities. They're capabilities that a country or organisation that is small but relatively technologically advanced can gain quite quickly.

This is part of what we've seen in Ukraine. Ukraine has been able to improve its cyber capabilities very quickly. Despite its smaller set of resources to draw on relative to Russia, Ukraine has been able to upskill in a way that has allowed it to use a variety of cyber techniques to support its objectives in the war. And Ukraine has been able to be relatively successful with these attacks despite some of those initial limitations.

Do you think cyber warfare is changing the balance of power on the world stage?

Cyber warfare affects the balance of power because it has this unique asymmetric quality where states that might be traditionally weaker in some domains can develop comprehensive cyber warfare capabilities. When we look at the broader space of cyber conflict, we see actors like North Korea that are relatively sophisticated despite not having large powerful militaries or having the same sort of strong economic capacity.

As the technology sector becomes increasingly important both economically and to improving military capabilities, states that have more advanced technological capabilities will become more influential. We see this not just when we're talking about offensive cyber operations or cyber war, but even the most basic conventional technologies today are often complemented by an important suite of connected cyber capabilities.

Whether that's communications or command infrastructure or connections to intelligence gathering capabilities, those supplemental assets that rely on the cyber domain and the space domain can really enhance the ability of a military to project power and to engage in war fighting.

This means part of the competition moving forward will not just be about how many weapons a state has but how precise, how accurate and how sophisticated those systems are. And those questions for the most part are technological questions.

When we see headlines in the media about cyberattacks, grids being shut down, traffic lights being stopped, things like that, how realistic are they? Should we be scared?

Many countries have the ability to use some combination of cyber and other techniques to affect major infrastructure, whether that's something like an electric grid or a water treatment plant. We've even seen cases where these technologies are identified or there are attempts to use them and they're able to be stopped.

The fact that this technology is there means if we were to see large scale conflict, let's say a war between very technologically advanced countries with large militaries, that war could be much more dangerous and expansive than it would be in the absence of those cyber technologies.

But what we often see in the media is more this fear of a bolt from the blue. Tomorrow you're going to wake up and there'll be no internet. It's not something that really states have any incentive to do except in the most extreme circumstances.

This fear isn't new. In the Cold War, we often saw a similar worry that you'd wake up tomorrow to a large-scale nuclear war, but that's not how conflict starts. You have crises, the tensions escalate, they become low-level conflict. Eventually they move up to these larger more dramatic effects. Cyber warfare is part of that long history of escalation.

This interview features extracts from Will the next World War be a cyberwar?, an LSE iQ podcast episode.

Note: This article gives the views of the interviewee, not the position of LSE European Politics or the London School of Economics.

Image credit: MMD Creative provided by Shutterstock.

About the author

Lauren Sukin

Dr Lauren Sukin is the John G. Winant Associate Professor in US Foreign Policy in the Department of Politics and International Relations at the University of Oxford as well as a Professorial Fellow at Nuffield College at the University of Oxford.

Charlotte Kelloway

Charlotte Kelloway is Media Relations Manager at the London School of Economics and Political Science.

Posted In: LSE Comment | Politics | Russia-Ukraine War