SPEECH

Lindy Cameron at Chatham House security and defence conference 2022

Lindy Cameron discusses the cyber dimension of the Russia-Ukraine conflict in keynote speech.

The National Cyber Security Centre's CEO Lindy Cameron delivered a keynote speech at the Chatham House security and defence conference 2022.

Lindy Cameron discussed the cyber dimension of the Russia-Ukraine conflict, focusing on what the NCSC has observed and the UK's response.

Following her keynote speech, Lindy Cameron took part in a panel discussion on the topic of how cyber considerations reshape transatlantic security thinking alongside Madeline Carr (Professor of Global Politics and Cyber Security, UCL), Heli Tiirma-Klaar (Director of Digital Society Institute, ESMT Berlin) and Jamie Shea CMG (Associate Fellow, International Security Programme, Chatham House).

The full speech is available below.

Lindy Cameron's keynote speech in full

Good afternoon and thank you for inviting me.

As we approach the first winter of the Russian invasion of Ukraine, Russia's physical brutalities are clear for all to see. I also want to continue to illuminate the dark corners of Russia's digital campaign.

As CEO of the UK's National Cyber Security Centre, I will focus on the cyber component of this conflict – sharing our observations and understanding of what has happened, as well as highlighting the measures we can all take to secure our digital future.

Tracking Russia

Since President Putin came to power, we have seen an increasingly aggressive and reckless Russian approach to foreign policy and casual disregard of international law.

From the poisoning of Sergei and Yulia Skripal to the bloody conduct in the Syrian Civil War and much in between.

Since its establishment in 2016, a primary focus of the NCSC has been tracking and defending against the threat posed by state actors, including Russia.

But our efforts go back much further than that. For decades, our parent organisation GCHQ has been studying Russian doctrine and tracking the threat Russia poses in the cyber domain. Over this period, Russia has invested significantly in its cyber capabilities – and has used it as a means of projecting power.

This has given us a deep understanding of the Russian threat in cyberspace, both by state and non state actors. That does not necessarily make attacks simple to counter, but it does allow the UK to draw upon these unique insights and capabilities to act responsibly in cyberspace, and to more effectively defend itself and its allies, in the digital realm.

Ukraine background

To understand Russia's invasion of Ukraine, we have to begin by looking back over the last decade.

In 2014, Putin's illegal annexation of Crimea was accompanied by cyber activity. Alongside the invasion, he instigated a cyber-enabled information campaign, encouraging Russian speakers to vote for annexation and then set loose a series of botnets to attack Ukrainian infrastructure and government targets.

While the Minsk II ceasefire reduced the kinetic warfare, it did not prevent Russia's sustained pairing of cyber and information warfare against Ukraine. The most notable attacks, in 2015 and 2016, of the Ukrainian power grid caused massive power outages in the depths of winter. But these were just the most prominent – Ukraine was on the receiving end of fairly constant attacks from Russia.

Then in 2017 Russia launched the destructive NotPetya cyber attack, which affected Ukraine's financial, energy and government institutions.

But NotPetya's indiscriminate design caused it to spread further, affecting other European and Russian businesses, and causing billions of dollars' worth of damage.

This kind of collateral damage is the risk of careless and irresponsible use of cyber capabilities, and this kind of uncontained spillover was one of the risks we were most concerned about earlier this year in the run up to the invasion of Ukraine.

Russian global cyber operations

While the principal focus of this speech is on the cyber dimensions of the Russian invasion of Ukraine, it's worth briefly reflecting on the fact that Russia's cyber activity is not solely focused on Ukraine.

Russia runs highly sophisticated, global cyber operations against the UK and our allies – and has done for decades. The SolarWinds compromise in 2020 is a good example of the espionage threat that we face. While less destructive than some of the incidents I will go on to describe – these cyber campaigns are designed to undermine our national interest and that of our allies and so should be vigorously defended against.

Ukraine 2022

This brings us to Russia's invasion of Ukraine in February this year.

As Jeremy Fleming, the Director of GCHQ, has articulated recently in his Economist article, Putin's struggle for influence extends beyond the physical battlefield.

Putin's online disinformation campaign was designed to cause confusion and chaos, while his cyber attacks sought to undermine confidence in the Ukrainian leadership.

Both efforts have largely failed, thanks to the efforts of Ukrainian and Western digital expertise within governments and the private sector.

The release of intelligence by the UK and our Allies enabled us to get ahead of Putin false flag operations and disinformation narratives, while staunch, professional and effective cyber defences have disrupted Russia's clumsy efforts to deploy offensive cyber measures in Ukraine.

This is not to say that cyber activity has not featured in this war. Far from it.

Both sides are using cyber capabilities to pursue their aims. Both sides understand the potential of integrating cyber and information confrontation with their military effort.

What have we seen?

We haven't seen 'cyber Armageddon'. But that's not a surprise to cyber professionals, who never expected it. What we have seen is a very significant conflict in cyberspace - probably the most sustained and intensive cyber campaign on record – with the Russian State launching a series of major cyber attacks in support of their illegal invasion in February.

Prior to the invasion, the GRU launched multiple DDoS attacks against Ukrainian government websites and its financial sector. This happened alongside the deployment of Whispergate and HermeticWiper wiper malware.

And this was followed on 24 February by the attack against ViaSat, an American commercial satellite internet company. The primary target was the Ukrainian military, but thousands of personal and commercial internet users were affected, including wind farms in central Europe. While not as damaging as the spill over from NotPetya, this clearly shows that the use of cyber in warfare can go beyond the borders of the countries involved.

I could go on, but most of this is a matter of public record, so it's probably more beneficial to tell you what we make of all this.

What do we make of it?

Firstly, and most importantly, we have not been surprised by the volume of Russian offensive cyber operations, nor have we been surprised by their targeting.

It fits our understanding of Russian doctrine – integrating cyber operations alongside real world offensive actions.

Russian cyber forces from their intelligence and military branches have been busy launching a huge number of attacks in support of immediate military objectives.

While these attacks may not have been apocalyptic in nature, this was not necessarily their purpose. Their actions suggest a clear rationale to reduce the Ukrainian Government's ability to communicate with its population, impact the Ukrainian financial system at a time of heightened concern and divert Ukrainian cyber security resource from their other priorities.

Attacks such as ViaSat were more sophisticated, but the goal was similar - disable or downgrade the Ukrainian government's ability to communicate. Russia launched this cyber attack one hour before its physical military attacks against Ukraine – a visible example of Russian doctrine in action: using cyber operations as a tool in support of wider military objectives.

One specific observation is that Russia has favoured wiper malware. Much like ransomware, this encrypts a device, making its data inaccessible. But, unlike ransomware, the effect is not designed to be undone. Thus, the infected device is rendered useless. Obviously, there would be dire consequences globally if such malware propagated in the same way NotPetya did.

Ukrainian defence

But for me, in many ways the most important lesson to take from the invasion is not around the Russian attacks – which have been very significant and, in many cases, very sophisticated. It is around Russia's lack of success.

Try as they might, Russian cyber attacks simply have not had the intended impact.

This lack of Russian success could be considered unexpected. However, the reasons for it can be attributed to three elements: impressive Ukrainian cyber defences, incredible support from industry partners and impressive collaboration between the UK, US, EU, NATO and others.

Just as we have seen inspirational and heroic defence by Ukrainian military on the battlefield. We have seen incredibly impressive defensive cyber operations by Ukrainian cyber security practitioners.

Many commentators have suggested that this has been the most effective defensive cyber activity undertaken under sustained pressure in history.

In many ways, Russia has made Ukraine match fit over the last ten years by consistently attacking them.

Of course, the UK has provided support. For several years, the UK has supported Ukraine to improve their resilience against cyber threats. This has included measures to enhance their incident response, forensics, and assessment processes.

The UK has also dedicated significant resources to enable others to better monitor and understand Russia's cyber threats. This intelligence is shared with our allies and others subject to Russia's malign cyber interference in their sovereignty, so that we are all better prepared.

But if the Ukrainian cyber defence teaches us a wider lesson – for military theory and beyond – it is that in cyber security, the defender has significant agency. In many ways you can choose how vulnerable you can be to attacks.

This activity has provided us with the clearest demonstration that a strong and effective cyber defence can be mounted, even against an adversary as well effective cyber defence can be mounted, even against an adversary as well prepared and resourced as the Russian Federation.

UK response

There is a huge amount that countries – and organisations for that matter – can learn from the Ukrainian cyber defence about preventing cyber attacks from taking hold or minimising the impact if they do get through.

Central to this is a commitment to long term resilience.

Building resilience means we don't necessarily need to know where or how the threat will manifest itself next. Instead, we know that most threats will be unable to breach our defences. And when they do, we can recover quickly and fully.

Since the start of the year, the NCSC has been advising UK organisations to take a more proactive approach to cyber security, in light of the situation in Ukraine.

Effectively, we said organisations should be operating at a heightened threat level. This includes taking measures such as verifying all software is up to date, checking backups and preparing an incident plan. You can find this advice on our website at www.ncsc.gov.uk

But there may be organisations that are beginning to think "is this still necessary?" as in the UK we haven't experienced a major incident related to the war in Ukraine. My answer is an emphatic "yes."

In response to significant battlefield set-backs, in the last week we have seen Putin react in unpredictable ways. So, we shouldn't assume that just because the conflict has played out in one way to date, it will continue to go the same way.

There is still a real possibility that Russia could change its approach in the cyber domain and take more risks – which could cause more significant impacts in the UK.

We have already seen – in the case of ViaSat – the conflict causing significant impact outside the borders of Ukraine.

And increasing organisational resilience in response to the threat from Russia doesn't just increase resilience to attacks from Russia, it raises the bar against all threats, such as criminally motivated ransomware, in a non-escalatory way.

So UK organisations – and their network defenders – should be prepared for this period of elevated alert to be with us for the long haul. Across the UK, we need to focus on building long-term resilience. Just as the Ukrainian defenders have done.

True resilience is a marathon not a sprint.

Unified partnerships

Along with resilience comes the need for a united front.

The pooling of resources among friends and allies is what will enable us to stay ahead of the threats and protect the freedoms and security of the digital age in which we live.

Our open, collaborative approach gives us a natural advantage. It encourages innovation, spurring the creation of an ecosystem which evolves naturally to defend against any and all threats.

This is not a simply an alliance of governments. The private sector is also deeply entrenched in the defence of Ukraine.

From my perspective, the private sector has an increasingly critical role to play in cyberspace, and Ukraine has demonstrated the advantage that public-private partnerships afford to hardening cyber defences.

Indeed, Russian actors face a formidable force from cyber experts in the UK, US, EU and other allied nations who are frustrating their activity. It's a strong ray of hope for the future.

Conclusion

So, looking back to the start of the year, we can't help but be impressed by the hugely effective defence that the Ukrainian network defenders have mounted.

They have been true heroes and have saved lives in the face of sophisticated and sustained Russian cyber aggression.

But it’s vital that we learn the lessons that Ukraine learnt over the last decade. We need to invest in resilience – right across the UK.

This remains an urgent challenge. Despite not being as successful as Putin would have liked, Russia remains a very sophisticated cyber power.

Thank you for your time.

PUBLISHED

28 September 2022

DATE OF SPEECH

28 September 2022

LOCATION

Chatham House, London

WRITTEN FOR

Public sector

Large organisations

Cyber security professionals