How close is a full-blown global cyber war after Russia's attack on Ukraine?

Irene Tham
Tech Editor

SINGAPORE - As Russian tanks rolled into Ukraine's capital Kyiv late last week in the biggest invasion in Europe since World War II, a full-blown cyber war is threatening to inflict collateral damage globally.

Last week, the United States warned businesses to watch for ransomware attacks after Western powers imposed unprecedented economic sanctions targeting Russian banks, oil refineries and oligarchs, including even Russian President Vladimir Putin himself.

British firms have also been warned to shore up their digital defence over concerns of possible Russian cyber attacks. Of concern is Britain's critical infrastructure supplying energy, water, transportation, health and telecommunications services, which had vulnerabilities known to be exploited by Russian hackers.

On Sunday (Feb 27), the Singapore Computer Emergency Response Team (Singcert) warned organisations here to be on heightened alert against possible cyber attacks.

Many questions have surfaced since. Is the threat real? How might cyber warfare be deployed, and what kind of damage can it do?

What is cyber warfare?

Cyber warfare is waged with stealth. Bullets and bombs take the form of malware and spurious information requests in a distributed denial-of-service (DDoS) attack to take down computers. It is hard to tell who the threat actors are.

Notably, there has never been a massive cyberwar happening alongside military combat in the real world - until now.

Last Wednesday, the websites of several Ukrainian banks and government departments were taken offline after a DDoS attack overwhelmed systems with bogus requests.

Ukraine's State Service of Special Communication and Information Protection also said it had observed phishing attacks on public authorities and critical infrastructure, as well as attempts to penetrate private sector networks.

Last week, Slovakia-based cyber-security firm ESET and American cyber-security firm Symantec discovered a new strain of computer-disabling malware on hundreds of machines in Ukraine, Latvia and Lithuania.

Hackers also took down the website of state-run TV network Russia Today last Thursday and Friday in another DDoS attack.

This is just the tip of the iceberg, experts said.

"It's... important not to misjudge the purpose of these attacks - the disruption they cause is designed to intimidate and undermine and is not an end to itself," said Mr John Hultquist, an expert on Russian cyber operations at American cyber-security firm Mandiant.

"Furthermore, they may be timed or accompanied by other elements to magnify their psychological impact," he said.

What kind of damage can cyber warfare do?

Warring nations could shut down each other's power grids and other essential services, and interfere with the safe operations of critical infrastructure such as dams and nuclear power plants.

In 2007, a massive DDoS attack believed to be linked to Russia disrupted e-government and e-banking services in the Baltic state of Estonia for weeks.

In the winter of 2015, power supply to about 700,000 homes in Western Ukraine was abruptly cut off for up to six hours due to what was believed to be the work of Russian hackers. It took months for the control centres to be fully operational again.

Less than a year later in 2016, the lights faded again in Ukraine's capital city of Kyiv because of malware that erased its power grid's system commands.

Most recently in May last year, top ransomware group Conti's attack on Ireland's healthcare system shut down the latter's hospital appointment and X-ray systems for weeks. There were also delays in Covid-19 testing as a portal to capture the testing data went out. The attack is reportedly costing the country's hospitals more than US$100 million (S$135 million) in recovery.

Disinformation campaigns and fake news such as the ones said to be funded by Russia to sway votes in the 2016 US presidential election is another type of cyber warfare that is no less insidious.

Why worry, and why now?

Cyber warfare is a recurring and chronic issue. Rival powers have spied on one another, stolen secrets and spread misinformation for decades.

But cyber warfare has traditionally operated in the grey area between peace and war. Now, the threat of a full-blown attack has gone up by a few notches as some vigilantes have started to take sides in the Russia-Ukraine conflict to start a proxy war.

Already, two top ransomware groups and hacktivist group Anonymous last week said they were getting involved in the conflict.

Members of Anonymous said on Twitter that they would be launching attacks against the Russian government. Russia Today blamed Anonymous for its service disruption.

In the opposite camp were Conti and CoomingProject, which support the Russian government and suggested they would strike in response to American cyber aggression.

Britain-based cyber-security firm Sophos' principal research scientist Chester Wisniewski said on the firm's website last week that the declarations increased the risk for everyone, including those not involved in the conflict.

"Vigilante attacks in either direction increase the fog of war and generate confusion and uncertainty for everyone," Mr Wisniewski said.

How real is the collateral damage?

Senior fellow Benjamin Ang at the S. Rajaratnam School of International Studies (RSIS) in Nanyang Technological University said that the threat of cyber attacks spilling over to other countries is not to be dismissed.

"Just look at the NotPetya malware in 2017. It has been called a Russian cyber attack targeting the Ukraine, but it spread, intentionally or not, all over the world," said Mr Ang, who heads the school's cyber and homeland defence programme.

Ransomware NotPetya was unleashed on Ukraine's financial sector in 2017, and ended up spreading to millions of computers all over the world, resulting in damages in the billions of dollars as operations and services ground to a halt.

Russia's top oil producer, Rosneft, and the Ukrainian government were among the first to be hit. Other operations affected included India's largest container operation, the Jawaharlal Nehru Port Trust, pharmaceutical giant Merck's US facilities, and a Cadbury chocolate factory in Australia.

In its advisory, Singcert urged businesses to turn on multi-factor authentication for all remote, privileged and administrative access to their network. Systems should also be updated with the latest firmware, security patches and anti-software. Corporate networks should be scanned at least once a week for breaches.

Are there any rules that govern such cyber warfare?

The Geneva Conventions and other international treaties have set out legal standards for humanitarian treatment in a traditional war. The rules apply only in times of armed conflict and seek to protect people who are not or no longer taking part in hostilities, including civilians, prisoners of war and armed forces who are sick and wounded.

However, the threshold for when cyber attacks cross the line is often unclear, although some brief discussions on definitions have taken place.

In 2014, North Atlantic Treaty Organisation (Nato) leaders agreed that a cyber attack could trigger Article 5 of their founding treaty, in which an attack on one ally is treated as an attack on all allies, justifying a collective defence. In 2016, Nato leaders designated cyberspace as a "domain", alongside land, sea and air in a time of conflict.

But Nato has yet to invoke Article 5's collective defence mechanism on a cyber attack. "There are good reasons to be cautious - as long as cyber attacks only delete data or cause disruptions, but do not cause injury, death or physical damage," said RSIS' Mr Ang.

Plus, it is not clear whether international law will classify cyber attacks as armed attacks that justify armed retaliation, he added.

The first time that a military retaliated with physical violence against a cyber attack was in 2019, when Israel bombed a building in Gaza to foil an attempted cyber attack on Israeli systems by Hamas, the Islamist Palestinian group that controls the territory.

Mr Ang said that the legal standards for humanitarian treatment in a physical war should also apply in cyberspace.

"Many countries would argue that civilian targets like hospitals should not be cyber attacked," he said. "The grey area is facilities that serve both the military and civilians, like power plants."

But tracking down aggressors in cyberspace may not be so easy.

"Even if cyber attacks have physical effects, the accused state may escape responsibility, having covered their tracks or used proxies like cybercrime gangs," he added.