Protection over privacy

Ukraine's plan to stem a surge in cyberattacks sparks privacy fears.

By UMBERTO BACCHI

FROM crashing supermarket tills to messing with radiation readouts, Ukraine is hoping to tackle an ever-growing list of cyberattacks with a new law that rights experts warn could give authorities excessive powers to pry into the lives of citizens.

Last month, a group of lawmakers led by members of the ruling party proposed a set of laws that would, among other things, boost police search powers and require Internet firms to store and provide access to large amounts of user data.

"If these draft laws are passed, then the state may have much easier access (to) the personal data of persons and ... their communications," said Maksym Dvorovyi, a lawyer at the Digital Security Lab, a Ukrainian digital rights group.

Since 2014, hackers have knocked out Ukraine's power supplies, frozen supermarket tills, affected radiation monitoring at the stricken Chernobyl nuclear power plant, and forced the authorities to prop up the hryvnia currency after the banks' IT systems crashed.

In 2019, a virus downloaded in a tax accounting program spread to wreak havoc around the globe, while only last month hackers forced the national police to temporarily shut down its website.

Reports of online scams and attacks against Ukraine's government ministries and information portals can run into the thousands every month, according to a report released by the US State Department in August.

And the number of incidents has increased during the coronavirus pandemic, with many daily activities moving online, Denis Monastyrsky, a lawmaker with the ruling Servant of the People party, said in emailed comments.

From March to May, authorities recorded about 15,000 cyber incidents and 88,000 "suspicious events", he said, adding that Internet fraud, phishing – a cyberattack that tricks users into disclosing sensitive information – and fake online news were also on the up.

"The main purpose of these draft laws is to increase the capacity of law enforcement agencies in the fight against cybercrime," said Monastyrsky, who initiated the reform and heads a parliamentary committee on law enforcement.

With Ukraine regarded by some cybersecurity experts as a guinea pig for Russian state-sponsored hacks, despite Kremlin denials, even rights groups and members of the opposition concur that the country's cybersecurity laws need updating.

The proposed changes seek to bring legislation in line with the Council of Europe's Convention on Cybercrime, for example, by regulating for the first time the use of electronic evidence in criminal proceedings.

Dvorovyi at the Digital Security Lab said this would be a positive step for the country's courts.

Now courts often have to use cumbersome legal manoeuvres to handle electronic information during a case, such as asking lawyers to load a webpage on their laptop and show it to the courtroom for it to be admitted as evidence, he explained.

The new law lists webpages, as well as digital documents, photos, videos, virtual assets and other electronic information as evidence that is admissible in court and can be presented in their original form or as a copy.

This would also allow for cryptocurrencies obtained as the result of criminal activities to be confiscated – something that is not currently possible, added Monastyrsky, the lawmaker.

While the proposed amendments would do little to prevent attacks, which would require strengthening cybersecurity infrastructure, they could help investigating them and bringing those responsible to justice, said Dvorovyi.

Yet, privacy campaigners and tech experts have raised concerns that some of the proposed amendments might go too far.

One provision would allow detectives and prosecutors to access information stored on laptops, smartphones and other devices if they see fit during a search, with no need for a specific warrant.

But this lack of oversight could be problematic in a country long regarded as riddled with corruption, said Kira Rudyk, head of the opposition party, Golos.

She noted that personal databases are easily sold online in Ukraine and even wiretaps – which require a warrant – are often abused.

Another measure would oblige Internet providers to store everyone's web traffic information for 12 months and grant investigating authorities access to it, in some cases with no need for a court order, said Oksana Pokalchuk, head of Amnesty International Ukraine.

Dvorovyi, the digital rights lawyer, said this risks exposing users' data to leaks and hacks, and adds an unfair burden on service providers.

"It may demand the installation of extremely large servers on which such information will need to be stored," said Dvorovyi.

Such provisions are not unique.

In Britain, the Investigatory Powers Act – called the "Snoopers' Charter" by critics – which came into force in 2017, can also compel companies to store Internet history data for a year and grant access to the police and security services.

The law, which detractors argue gives authorities some of the most extensive snooping capabilities in the West, has been the object of numerous legal challenges from rights groups.

Ukraine's proposed reform has also come under fire from the Ukrainian Internet Association, representing more than 200 companies, which said the law would increase costs for consumers and harm small businesses with fewer financial resources.

Privacy campaigners have urged a rethink of the bills, which still have to be discussed and voted on by the relevant committees before going to parliament.

"Ukrainian legislation concerning cybersecurity needs to be modernised," said Pokalchuk of Amnesty.

"But we also call on Ukrainian authorities to take into consideration ... international obligations in the field of human rights."

Monastyrsky, the lawmaker, said most of the criticism was unfounded as the proposals comply with international treaties and Ukraine's constitution.

"In the mass media, there is only general criticism in the context of alleged violations of human rights, pressure on businesses. It is not true," he said. – Thomson Reuters Foundation