OSCE victim of 'major' cyber attack

December 28 2016, by Simon Sturdee

A Western intelligence agency believes that Russian hackers group APT28 was behind the attack on the Organization for Security and Co-operation in Europe (OSCE)

The Organization for Security and Co-operation in Europe, an international election and war monitor, said Wednesday it had become the latest global institution to suffer a "major" cyber attack.

The Vienna-based OSCE has its origins in the Cold War but after 1991 it expanded and now has 57 member states including the United States, Russia and Ukraine.

It currently has 700 monitors focused on the conflict in eastern Ukraine and is also active in observing elections and tracking media freedom.

OSCE spokeswoman Mersiha Causevic Podzic told AFP in an email that it "became aware of a major information security incident" in early November.

The attack "compromised the confidentiality" of the organisation's IT network and put "its integrity at risk", although it was still able to operate, she said.

According to French daily Le Monde, which first reported the incident, a Western intelligence agency believes that Russian hackers group APT28 was behind the attack.

This group, also known as Pawn Storm, Sofacy and Fancy Bears, is believed to be behind other high-profile cyber attacks and to be linked to Russia's security services.

The OSCE said "the way in which the attacker accessed the OSCE was identified, as have some of the external communication destinations".

France's ambassador to the OSCE played down the dangers from the attack, saying officials in Vienna—long seen as a hotbed of espionage—are trained to be aware to the risks.

"Diplomats at the OSCE are warned that attempted spying, in whatever form, are part and parcel of this organisation," Veronique Roger-Lacan told AFP.

The cyber frontier

But cyber attacks by criminals and governments are on the rise, with states and firms spending billions of dollars to defend and arm themselves.

The issue has become contentious between the United States and Russia, with the latter alleged to have hacked party computers and leaked documents during the US election campaign.

The White House has said Russian President Vladimir Putin was directly involved and President Barack Obama has vowed Washington will retaliate "at a time and place of our own choosing".

The Kremlin has rejected the accusations, demanding America presents proof. US President-elect Donald Trump has dismissed the claims as "ridiculous".

In Europe, with Germany holding elections late next year, Chancellor Angela Merkel and other top officials have warned that the country could be the target of Russian cyber attacks.

France announced its first cyber-warfare army unit this month, mirroring plans drawn up by Britain, which launched a cyber-defence plan backed by 2.1 billion euros ($2.2 billion) of funding.

It is not just Russia that is seen as a threat in the West.

North Korea has already proved it is a player with a damaging attack on South Korean banks and broadcasters in 2013. The US also blamed Pyongyang for an audacious hack on Sony Pictures the following year.

Russia too has been a victim. Earlier this month its telecom operator said

that it had blocked a series of cyber attacks on the country's leading banks.

And in the Middle East, the United States and Israel are thought to have been behind the Stuxnet worm that sabotaged Iran's nuclear infrastructure in 2010.

Firms in the West have also been targeted. In Germany, almost a million Deutsche Telekom customers were knocked offline in late November after the firm was hit by hackers.

In September US internet giant Yahoo revealed that it had been the victim of one of biggest thefts of online users' personal information ever, affecting some 500 million accounts.