Israel facing 'millions' of cyber-attacks over Gaza (Update)

November 18 2012, by Dmitry Zaks

A picture of the Tel Aviv Stock Exchange building in the Mediterranean city of Tel Aviv on January 16, 2011. The Israeli government on Sunday admitted it had become the victim of a mass cyber-warfare campaign with millions of attempts to hack state websites since the start of its Gaza offensive four days ago.

Israel admitted Sunday it has been targeted in a mass cyber-warfare campaign that has witnessed millions of attempts to hack state websites since the start of its Gaza offensive four days ago.

Finance Minister Yuval Steinitz told reporters the government had been forced to wage war on "a second front"—of cyber attacks against Israel.

"This is an unprecedented attack," Steinitz said, indicating that Israel had "deflected 44 million cyber attacks on government websites" since it began a widespread air campaign over Gaza on Wednesday.

"All the attacks were thwarted except for one, which targeted a specific website that was down for six or seven minutes," he said.

The comments from Israel's overseer of Internet security came a day after the Anonymous online activist group claimed downing dozens of websites of state agencies and a top bank in protest over the Jewish state's deadly air assault.

It also coincides with both Israeli and Palestinian attempts to exploit the social networks to win over public opinion amid the worst outbreak of Middle East violence in four years.

Steinitz did not say who was responsible.

But he said the government had fended off almost every attack, with analysts pointing out that the Jewish state has sophisticated protection that shields its online assets.

Anonymous on Saturday claimed it had downed or erased the databases of nearly 700 Israeli sites that included the powerful Bank of Jerusalem finance house.

It also claimed to have briefly downed the foreign ministry website in protest over an alleged Israeli threat to cut Gaza's Internet access.

"For far too long, Anonymous has stood by with the rest of the world

and watched in despair the barbaric, brutal and despicable treatment of the Palestinian people in the so called 'Occupied Territories' by the Israel Defence Force," it said in a statement.

"But when the government of Israel publicly threatened to sever all Internet and other telecommunications into and out of Gaza they crossed a line in the sand."

Steinitz made no direct reference to Anonymous, but stressed the Israeli government had a backup plan for "essential websites" should they be taken down.

Analysts said Israel was a frequent target of cyber-warfare even during times of peace and was therefore prepared better to deal with campaigns like the one this week.

"Nothing will happen to Israel because this attack is bound to fail," said Tal Argoni, a cyberwarfare expert at the Tel Aviv-based firm, 2BSecure.

Argoni said Israel had developed a system whereby websites which detect an attack automatically become inaccessible to foreign addresses, while operating normally for locals who are unaware that anything is wrong.

"This makes the foreigners think that their distributed denial of service (DDoS) attack was working when it really is not," Argoni said.

"And that makes them stop their DDoS attack before it has accomplished anything."

But Professor Danny Dolev of the Hebrew University of Jerusalem said that much remained undiscovered about how nations waged cyberwarfare against each other.

"Right now, what we have are attacks that are a nuisance but which have to be taken care of. But, what if the entire financial system is attacked?" he asked.

"This front is still very immature and there is still a lot more to be done."

(c) 2012 AFP