theguardian

Russia accused of unleashing cyberwar to disable Estonia

• Parliament, ministries, banks, media targeted • Nato experts sent in to strengthen defences

Ian Traynor in Brussels

Thursday 17 May 2007 02.32 BST

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

While Russia and Estonia are embroiled in their worst dispute since the collapse of the Soviet Union, a row that erupted at the end of last month over the Estonians' removal of the Bronze Soldier Soviet war memorial in central Tallinn, the country has been subjected to a barrage of cyber warfare, disabling the websites of government ministries, political parties, newspapers, banks, and companies.

Nato has dispatched some of its top cyber-terrorism experts to Tallinn to investigate and to help the Estonians beef up their electronic defences.

"This is an operational security issue, something we're taking very seriously," said an official at Nato headquarters in Brussels. "It goes to the heart of the alliance's modus operandi."

Alarm over the unprecedented scale of cyber-warfare is to be raised tomorrow at a summit between Russian and European leaders outside Samara on the Volga.

While planning to raise the issue with the Russian authorities, EU and Nato officials have been careful not to accuse the Russians directly.

If it were established that Russia is behind the attacks, it would be the first known case of one state targeting another by cyber-warfare.

Relations between the Kremlin and the west are at their worst for years, with Russia engaged in bitter disputes not only with Estonia, but with Poland, Lithuania, the Czech Republic, and Georgia - all former parts of the Soviet Union or ex-members of the Warsaw Pact. The electronic offensive is making matters much worse.

"Frankly it is clear that what happened in Estonia in the cyber-attacks is not acceptable and a very serious disturbance," said a senior EU official.

Estonia's president, foreign minister, and defence minister have all raised the emergency with their counterparts in Europe and with Nato.

"At present, Nato does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country," said the Estonian defence minister, Jaak Aaviksoo.

"Not a single Nato defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future."

Estonia, a country of 1.4 million people, including a large ethnic Russian minority, is one of the most wired societies in Europe and a pioneer in the development of "e-government". Being highly dependent on computers, it is also highly vulnerable to cyber-attack.

The main targets have been the websites of:

· the Estonian presidency and its parliament

· almost all of the country's government ministries

· political parties

· three of the country's six big news organisations

· two of the biggest banks; and firms specializing in communications

It is not clear how great the damage has been.

With their reputation for electronic prowess, the Estonians have been quick to marshal their defences, mainly by closing down the sites under attack to foreign internet addresses, in order to try to keep them accessible to domestic users.

The cyber-attacks were clearly prompted by the Estonians' relocation of the Soviet second world war memorial on April 27.

Ethnic Russians staged protests against the removal, during which 1,300 people were arrested, 100 people were injured, and one person was killed.

The crisis unleashed a wave of so-called DDoS, or Distributed Denial of Service, attacks, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers running the sites. The attacks have been pouring in from all over the world, but Estonian officials and computer security experts say that, particularly in the early phase, some attackers were identified by their internet addresses - many of which were Russian, and some of which were from Russian state institutions.

"The cyber-attacks are from Russia. There is no question. It's political," said Merit Kopli, editor of Postimees, one of the two main newspapers in Estonia, whose website has been targeted and has been inaccessible to international visitors for a week. It was still unavailable last night.

"If you are implying [the attacks] came from Russia or the Russian government, it's a serious allegation that has to be substantiated. Cyber-space is everywhere," Russia's ambassador in Brussels, Vladimir Chizhov, said in reply to a question from the Guardian. He added: "I don't support such behaviour, but one has to look at where they [the attacks] came from and why."

Without naming Russia, the Nato official said: "I won't point fingers. But these were not things done by a few individuals.

"This clearly bore the hallmarks of something concerted. The Estonians are not alone with this problem. It really is a serious issue for the alliance as a whole."

Mr Chizhov went on to accuse the EU of hypocrisy in its support for Estonia, an EU and Nato member. "There is a smell of double standards."

He also accused Poland of holding the EU hostage in its dealings with Russia, and further accused Estonia and other east European countries previously in Russia's orbit of being in thrall to "phantom pains of the past, historic grievances against the Soviet union and the Russian empire of the 19th century." In Tallinn, Ms Kopli said: "This is the first time this has happened, and it is very important that we've had this type of attack. We've been able to learn from it."

"We have been lucky to survive this," said Mikko Maddis, Estonia's defence ministry spokesman. "People started to fight a cyber-war against it right away. Ways were found to eliminate the attacker."

The attacks have come in three waves: from April 27, when the Bronze Soldier riots erupted, peaking around May 3; then on May 8 and 9 - a couple of the most celebrated dates in the Russian calendar, when the country marks Victory Day over Nazi Germany, and when President Vladimir Putin delivered another hostile speech attacking Estonia and indirectly likening the Bush administration to the Hitler regime; and again this week.

Estonian officials say that one of the masterminds of the cyber-campaign, identified from his online name, is connected to the Russian security service. A 19-year-old was arrested in Tallinn at the weekend for his alleged involvement.

Expert opinion is divided on whether the identity of the cyber-warriors can be ascertained properly.

Experts from Nato member states and from the alliance's NCSA unit - "Nato's first line of defence against cyber-terrorism", set up five years ago - were meeting in Seattle in the US when the crisis erupted. A couple of them were rushed to Tallinn.

Another Nato official familiar with the experts' work said it was easy for them, with other organisations and internet providers, to track, trace, and identify the attackers.

But Mikko Hyppoenen, a Finnish expert, told the Helsingin Sanomat newspaper that it would be difficult to prove the Russian state's responsibility, and that the Kremlin could inflict much more serious cyber-damage if it chose to.

More news

Topics

Russia Estonia Europe Cyberwar