

ARCHIVE | 2007 | 0517

Estonia accuses Russia of 'cyberattack'

NATO is investigating siege on Estonian government, media, and banking websites, but Russia denies involvement.

By Arthur Bright ▼ | MAY 17, 2007

 Save for later

Estonia accused Russia of launching a barrage of "cyberattacks" that are shutting down Estonian government, newspaper, and banking websites.

The **Guardian** reports that [the attacks began in late April](#), coinciding with Estonia's decision to move a Soviet World War II memorial, the Bronze Soldier, from a central location in Tallinn, the Baltic nation's capital. Though Estonians saw the memorial as a reminder of Soviet oppression, Russia viewed the decision to move it as an affront, prompting riots by ethnic Russians in Tallinn and condemnations and sanctions from Moscow. The cyberattacks have continued since then.

“ 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 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.

The Guardian notes that Estonia is a pioneer of "e-government" and one of the most wired countries in Europe, making it that much more vulnerable to cyberattacks. In order to stop the attacks, Estonia has shut down foreign access to the sites under siege.



Could you pass a US citizenship



SUBSCRIBE

Recommended: **Could you pass a US citizenship test?**

Estonian Foreign Minister Urmas Paet [accused the Kremlin of direct involvement](#) in the cyberattacks, saying they were an attempt to paralyze Estonian businesses and government offices, writes **The Times** of London.

“When there are attacks coming from official IP addresses of Russian authorities and they are attacking not only our websites but our mobile phone network and our rescue service network, then it is already very dangerous,” Mr Paet said.



TEST YOUR KNOWLEDGE | Could you pass a US citizenship test?

“It can cost lives. I hope they will stop it but the attacks are continuing. They are sending huge levels of stuff through the networks so that our different servers will crash.



PHOTOS OF THE DAY | Photos of the day 02/08

“The largest part of these attacks are coming from Russia and from official servers of the authorities of Russia.”

The **Guardian** reports that [Russia denies involvement](#) in the attacks.

“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.”

But technology news site **Ars Technica** writes that, [even if Russia is involved, such involvement may be impossible to prove](#). Mikko Hyppönen of F-Secure, a Finnish security company, said, “In practice there is just one IP address that leads to a government computer. It is of course possible that an attack was launched from there, too, but the person behind it could be anyone, from the son of some ministerial janitor upwards.”

The Economist notes, however, that instructions for DDoS attacks are being posted anonymously on Russian-language websites. Given Russia's potential involvement, NATO has given “[special attention](#)” to the cyberattacks.



FREE Newsletter

Get the Monitor stories you delivered to your in

- | | |
|----------------------------------|------------------------------|
| <input type="checkbox"/> Daily | <input type="checkbox"/> The |
| <input type="checkbox"/> BizTech | <input type="checkbox"/> Cha |
| <input type="checkbox"/> Science | <input type="checkbox"/> Boo |

“ "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?" asks a senior [NATO] official in Brussels. Estonia's defence ministry goes further: a spokesman compares the attacks to those launched against America on September 11th 2001. Two of NATO's top specialists in internet warfare, plus an American colleague, have hurried to Tallinn to observe the onslaught. But international law is of little help, complains Rein Lang, Estonia's justice minister.

Politics Foot
 Commentary C.S.I

Your e-mail address

Agence France-Presse writes that [part of the problem is the newness](#) of this kind of attack - rules on how to respond don't exist yet.

“ "We haven't yet defined what can be considered to be a cyber-attack, or what are the rights of member states and the obligations of EU and NATO in the event such attacks are launched," [Estonian Defence Minister Jaak Aaviksoo] said.

“ "The EU and NATO need to work out a common legal basis to deal with cyber attacks. For example, we have to agree on how to tackle different levels of criminal cyber-activities, depending on whether what we are dealing with is vandalism, cyber-terror or cyber-war," he said.

Hillar Aareleid, head of Estonia's Computer Emergency Response Team agreed, saying, "The unprecedented cyber-attacks against Estonia have clearly indicated we need much stronger regulations in this area. You could compare this with what our great-grandparents faced when cars first started to appear on the streets. Eventually, there were so many of them that new, strict rules needed to be implemented." ■



Next up



Moscow rattles Estonia with talk of 'concern' for its Russian population



PASSCODE
From Estonia, lessons for the Age of Cyberwar



Where are the cyberattacks? Russia's curious forbearance in Ukraine. (+video)

 Share
  Tweet
  E-mail
  More
  Print/Reprints

The CHRISTIAN SCIENCE MONITOR[®]

STAY CURRENT. GO FAR.
DISCOVER THE MONITOR DIFFERENCE

[f](#) [t](#) [g+](#)

[ABOUT](#) | [CONTACT US](#) | [SUBSCRIBE](#) | [E-READERS](#) | [ADVERTISE WITH US](#) | [CAREERS](#) | [FIND US ON](#)
[CONTENT MAP](#) | [TEXT](#) | [CORRECTIONS](#) | [REPRINTS & PERMISSIONS](#) | [MULTIMEDIA](#) | [A CHRISTIAN SCIENCE P](#)

© The Christian Science Monitor. All Rights Reserved. Terms under which this service is provided to you. Privacy Policy.

This ad is supporting your extension Downloads - Your Download Box: [More info](#) | [Privacy Policy](#) | [Hide on this page](#)