

Davos elites warned about catastrophic cyberattacks

January 24 2015



People have lunch during the World Economic Forum (WEF) annual meeting on January 24, 2015 in Davos, Switzerland

Attacks on power plants, telecommunications and financial systems, even turning all of Los Angeles' traffic lights green: Davos elites were warned Saturday of the terrifying possibilities of modern cyber terrorism.

Eugene Kaspersky, who heads the Kaspersky Lab security group, said the possibilities of individuals being hacked would only increase in future as more devices, such as "smart" televisions, are hooked up to the Internet.

"What you call the Internet of Things, I call the Internet of Threats," he told the assembled global political and business movers-and-shakers.

"The worst of the worst scenarios is an attack on a big infrastructure, a power plant. If there's no power, the rest of the world doesn't work," Kaspersky cautioned.

Estonian President Toomas Hendrik Ilves said that criminals could bring about chaos in a much lower-level way.

"You can wreak havoc in all kinds of ways," said Ilves, who added that it was the duty of governments to give citizens powerful encryption tools to protect their data.

He told an anecdote about traffic authorities in Los Angeles who went on strike and also set all the lights to red, sparking gridlock.

"But what if someone turned all the lights green?" he asked.

In the wake of the cyberhack on Sony late last year, cybersecurity has been a hot button topic at the four-day World Economic Forum in the swanky Swiss ski resort.

The conclusion, in Ilves's words: "Basically nothing is safe."

'The path to Hell'

Jean-Paul Laborde, head of the UN's counter-terrorism unit, pointed to

increasing links between organised crime and extremist groups such as Islamic State, which he said were now combining to launch cyberattacks on authorities.

"They even attack now ... in a low key way ... police infrastructure, in order to block police action against them outside their territories," said Laborde.

He called for an international legal framework to bring these criminals to justice but acknowledged it was "very, very difficult" to pin down their locations and agree common laws across nations.

Picking up on this theme, the Estonian president said that the line between government-sponsored attacks and [criminal activity](#) was becoming increasingly blurred.

"Governments pay criminals ... I call it the 'little Green Men-isation of cyber space'—you don't know who's doing it," he said, referring to the Russian "Little Green Men" secret service agents accused of engineering the annexation of Crimea last year.

With pressure mounting on Internet companies to block, for example, jihadist recruitment material on their networks, Bradford Smith, a top Microsoft executive, threw the ball back to public authorities.

"No one elected us. Isn't this the kind of decision that the US Congress or the French National Assembly were elected to make?" he asked.

Smith also warned of the dangers of putting in so-called "backdoors" to messaging systems, as urged recently by British Prime Minister David Cameron to keep track of potentially criminal activity.

"The path to Hell starts at the back door. You should not ask for back

doors. That compromises protection for everyone for everything," stressed the executive.

The World Economic Forum in Davos brings together some 2,500 of the top players in the sphere of finance, business and politics and ends later Saturday.

© 2015 AFP

Citation: Davos elites warned about catastrophic cyberattacks (2015, January 24) retrieved 8 May 2024 from <https://phys.org/news/2015-01-davos-elites-catastrophic-cyberattacks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.