Skip to navigation

Interesting Things

Things from around the world

February 24, 2010

Cyber Evil Will Thrive Without Global Rules — Good Luck With That

(http://www.wired.com/epicenter/2010/02/cyber-evil-will-thrive/)

Global "Rules" would probably make things easier for the bad guys instead of harder.

By Reuters (http://www.wired.com/epicenter/author/reuters/)

LONDON (Reuters) — The best weapon against the online thieves, spies and vandals who threaten global business and security would be international regulation of cyber space.

Luckily for them, such cooperation does not yet exist.

Better still, from a hacker's perspective, such a goal is not a top priority for the international community, despite an outcry over hacking and censorship and disputes over cyber space pitting China and Iran against Google.

Nations are thinking too parochially about their online security to collaborate on crafting global cyber regulation, an EastWest Institute security conference heard last week.

Policy statements from governments around the world are dominated by the need to heighten national cyber defenses. As a result, too many cyber criminals are getting a free ride.

"Nations are in denial," Indian cyber law expert Pavan Duggal told Reuters, saying national legislation was of limited use in protecting users of a borderless communications tool. "It may take a big shock of an event to wake people out of their complacency, something equal to a 9/11 in cyber space."

With a quarter of humanity connected to the Internet, cyber crime poses a growing danger to the global economy.

The FBI tallied $264 million in losses from Internet crime reported by individuals in the United States in 2008 compared to $18 million of losses from 2001: These were probably a fraction of the losses caused to companies and government departments.

The menace extends to many sectors including control systems for manufacturing, utilities and oil refining, since many are now tied to the Internet for convenience and productivity.

A priority for regulators is to find ways of tracking down criminals across borders and ensuring they are punished, a tough task when criminals can use proxy servers to remain anonymous.

Target the Perpetrator

"We cannot postpone the debate until we are in the midst of a catastrophic cyber attack," former U.S. Homeland Security Secretary Michael Chertoff told the conference. "We must formulate an international strategy and response to cyber attacks that parallels the traditional laws governing the land, sea, and air."

Security experts say the ability to conduct disastrous mass cyber attacks is the preserve of some governments, well beyond the capacity of militant guerrilla groups like al Qaeda. But it cannot be assumed that international organized criminal networks, long practiced at mass online fraud and theft, are not developing an interest in gaining this ability.

"Cyber crime is a very sophisticated crime with very sophisticated players and it takes a multinational effort to make sure we can enforce the law," Dell Services President Peter Altabef told Reuters. "Once you have identified who is at fault you really want to make sure, as a

deterrent, that you can go to those jurisdictions and enforce the laws on the books."

James Stikeleather, Dell Services Chief Technology Officer, told Reuters that tracking own criminals across borders could pose legal issues for drafters of multilateral regulation.

Giving an example, he said the more companies added the technology needed to give investigators the ability to attribute a crime, the more users' privacy and anonymity would be reduced.

"Playing With Fire"

"Probably the sticking point among the governments will be 'where is the appropriate level of attribution versus anonymity or privacy for what people are doing (online)'."

Datuk Mohammed Noor Amin, chairman of the U.N.-affiliated International Multilateral Partnership Against Cyber Threats, said failure to regulate could perpetuate cyber "failed states."

He cited impoverished countries where customers can purchase unregistered SIM cards with mobile Internet capability, giving them the ability to commit online crime such as identify theft against people in rich nations without fear of being traced.

He said it was in the interest of rich nations to help poorer countries develop the capacity to crack down on this kind of abuse, because their own citizens were being targeted.

"Governments tend to look at their self-interest. But it's actually in their own interest to collaborate," he said.

Altabef said the growing rate and scale of international cyber attacks threatened to undermine the trust between nations, businesses and individuals that was necessary for economies and societies to act on the basis of the common good.

Complacency was also a problem, delegates said. "Nations take for granted the Internet is going to be 'on' for the rest of our lives. It may not necessarily be so," said Duggal.

"Imagine the Internet being down for two to four weeks," he said. This would "rain disaster" on online businesses as well as transport, industry and governmental surveillance systems.

"People have realize the Internet is an integral part of every country, politically, socially and business-wise."

"Not to focus on cyber security is playing with fire."

(By William Maclean, Security Correspondent. Editing by Charles Dick)

Photo: Model of Britain's famed secret eavesdropping facility known as GCHQ (Government Communications Headquarters). Courtesy Gruntzooki (http://www.flickr.com/photos/doctorow/2686028409/)/Flickr

More From Reuters:

- China PLA officer urges new Internet control agency (http://www.reuters.com/article/internetNews/idUSTRE61L0OG20100222?rpc=40)
- Modern Etiquette:How to decline Facebook friends without offence (http://www.reuters.com/article/internetNews/idUSTRE61L1WL20100222?rpc=40)

More from Wired.com

- Web Banking to Upgrade Security (http://www.wired.com/techbiz/media/news/2005/10/69418)
- Yahoo Mail Security Flaw Exposes Passwords (http://www.webmonkey.com/blog/Yahoo_Mail_Security_Flaw_Exposes_Passwords)
- Hackers Take Down the Most Wired Country in Europe (http://www.wired.com/politics/security/magazine/15-09/ff_estonia)
- Google Hack Attack Was Ultra Sophisticated, New Details Show (http://www.wired.com/threatlevel/2010/01/operation-aurora/)
- Report Details Hacks Targeting Google, Others (http://www.wired.com/threatlevel/2010/02/apt-hacks/)
- Probe Traces Google Hack to Chinese Schools (http://www.wired.com/threatlevel/2010/02/probe-traces-google-hack-to-chinese-schools/)
- Google Hackers Targeted Source Code of More Than 30 Companies (http://www.wired.com/threatlevel/2010/01/google-hack-attack/)
- Conficker War Room! Your Front Row Seat for Cyber Armageddon (http://www.wired.com/threatlevel/2009/04/conficker-war-r/)
- Vote: Will Conficker Botnet Trigger 'Unthinkable Disaster' (http://www.wired.com/threatlevel/2009/03/will-conficker/)

http://www.wired.com/epicenter/2010/02/cyber-evil-will-thrive/ (http://www.wired.com/epicenter/2010/02/cyber-evil-will-thrive/)

You May Like

- 1. 14 Bathroom Inventions You Didn't Realize You Needed 6 months ago huffingtonpost.com Huffington Post HuffingtonPost.com (AOL) The

◎   Computer Tech, Reporting, Security, Social Networking, The World   ◎   0 Comments

Blog at WordPress.com. | The Highwind Theme.