Top US security agency turns to hackers for help

By ZHANG YUNBI
zhangyunbi@chinadaily.com.cn

The largest-ever hacker gathering in Las Vegas proved to be a perfect recruiting opportunity for the head of the US National Security Agency.

Keith Alexander, a four-star general and director of the US National Security Agency, took the stage in a black T-shirt and jeans on Friday to address the country's largest hacker convention, Defcon.

He delivered a recruiting pitch to the thousands in attendance, including hackers, professional defenders and researchers.

"You're going to have to come in and help us," said the spymaster. Alexander said privacy must be preserved, and new talent could help develop new tools.

The NSA also set up a special recruiting site during the convention.

"At NSA, we don't crack codes and develop new encryption algorithms just for the fun of it (but don't tell our tech teams that)," the website said.

The agency promised to guarantee the safety and security of new employees and their families, and said recruits must meet certain criteria to work at the NSA.

"It's true that you must be a US citizen, and you'll need a security clearance that requires a background investigation and polygraph," the NSA said on its website, adding that a few "indiscretions" in a recruit's past will not necessarily hurt their chances of being hired.

> **These days, Internet security and the crackdown on cyber crime are not just jobs for soldiers. Ordinary citizens of the community are also expected to join in the fight."**
>
> TENG JIANQUN
> RESEARCHER AT THE CHINA INSTITUTE OF INTERNATIONAL STUDIES

"You shouldn't automatically assume that you can't be hired. If you're really interested, you owe it to yourself to give it a shot."

Li Wei, Director of the Institute of Security and Arms Control Studies under the China Institute of Contemporary International Relations, said Washington is increasingly paying more attention to young hackers, some of whom could have promising careers.

"Some of them may become full-time employees of Washington's cyberspace forces, while others just find part-time jobs," Li said.

Alexander's appearance on Friday was regarded as a milestone for Defcon, "a hacker mecca with an often-uneasy relationship with the feds", CNN said.

The general's visit came after he was quoted by the New York Times as saying that between 2009 and 2011 there was a 17-fold increase in cyber attacks on critical US infrastructure such as power grids and mobile phone networks.

"My concern is destructive attacks with serious consequences on critical infrastructure (and key government systems)," said Alexander, who is also head of the US Cyber Command, which was created to defend against Internet-based attacks.

Alexander on Thursday told the Aspen Security Forum that some of the 17-fold increase was attributed to nation states and some to "hackers and other criminals".

Aside from the country's infrastructure, corporate businesses are also victims of cyber crime and online attacks against their online portals.

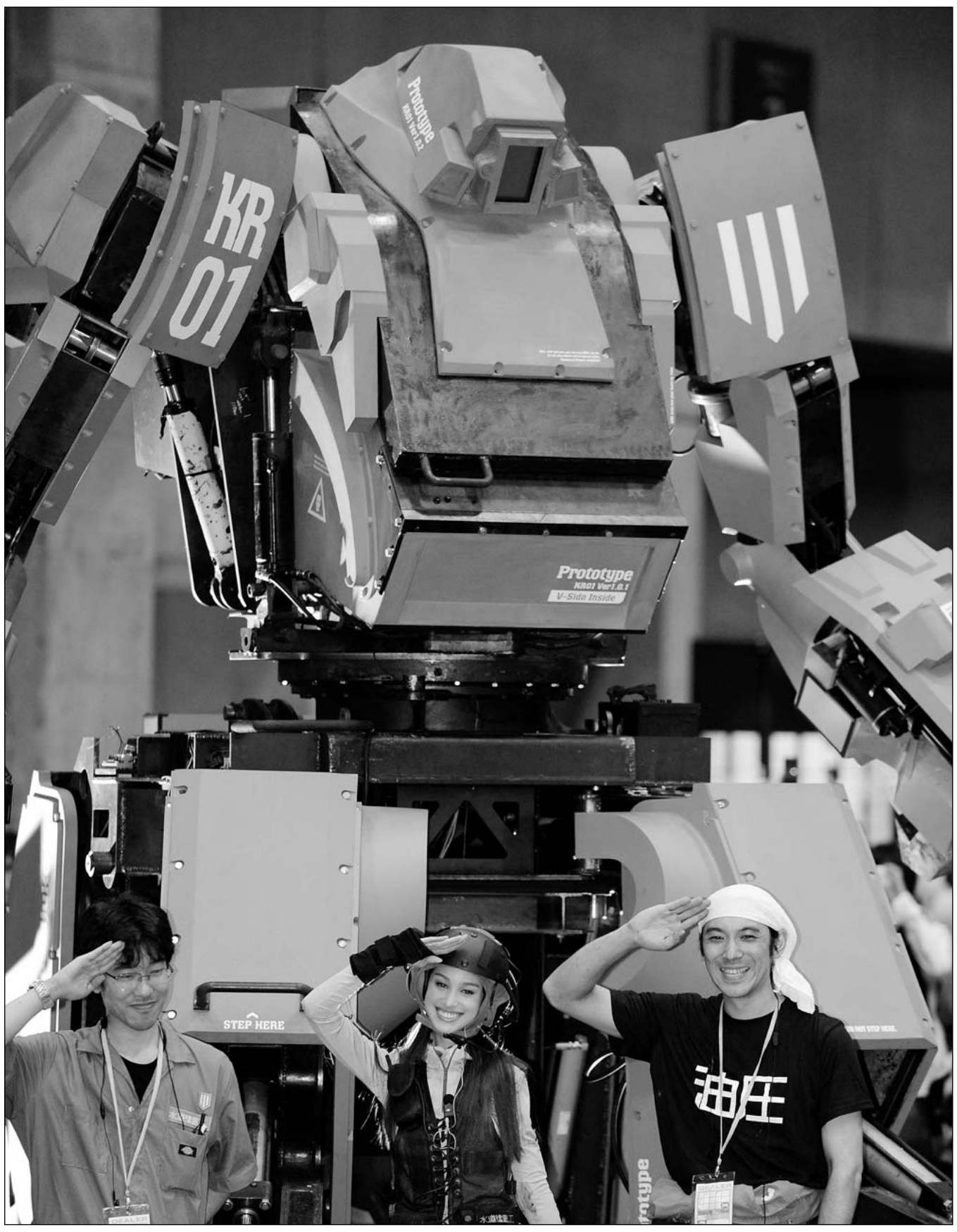
Washington's attempt to reach out to hackers not only serves its strategy for Internet security and cyber wars, but also the country's interest in information security, said Teng Jianqun, a researcher at the China Institute of International Studies.

"These days, Internet security and the crackdown on cyber crime are not just jobs for soldiers. Ordinary citizens of the community are also expected to join in the fight," Teng said.

Facebook, a leading social network company, announced before the Defcon's opening that it plans to widen its "bug bounty" program to reward researchers who spot holes in its corporate network, according to Bloomberg.

The company already pays a bug bounty to outside hackers who report weaknesses in its products.

Reuters contributed to this story.



REMOTE CONTROL ROBOT UNVEILED

PHOTO BY **YOSHIYAZU TSUNO** / AGENCE FRANCE-PRESSE

Engineers Wataru Yoshizaki (left), Kogoro Kurata (right) and "pilot" Anna salute in front of newly unveiled robot "Kuratas" at the Wonder Festival in Tokyo on Sunday. The robot, which measures four meters in height and weighs four tons, can either be controlled remotely through the 3G network or by a human seated within the cockpit.

West tightens Internet censorship, cybersecurtiy

By ZHOU WA
zhouwa@chinadaily.com.cn

In an age in which large-scale protests can be organized overnight via social media, or infrastructure networks can be shut down by hackers, Western countries are tightening Internet censorship and implementing tougher cybermonitoring policies.

While governments tend to play the national security card to defend plans for wider state access to email and digital communications, analysts and Internet users are concerned that unwatched cybermonitoring might tip the delicate balance between online security and state surveillance.

The United States Congress has recently revived a stalled cybersecurity bill that would allow information sharing between the private sector and the federal government to share threats and develop best practices and fixes.

The bill triggered a wave of protest from people who said it may harm the privacy of Internet users and still leave the country vulnerable to attacks, but the bill received support from US President Barack Obama, who urged congress to pass the Cybersecurity Act of 2012.

Although no one has managed to seriously damage or disrupt the critical infrastructure networks in the US, Obama said foreign governments, criminal syndicates and lone individuals are probing the country's financial, energy and public safety systems every day.

GOOGLE'S TRANSPARENCY REPORT DETAILING CENSORSHIP REQUESTS FROM GOVERNMENTS IN THE SECOND HALF OF 2011

Country	User information requests	Percentage where some or all information produced	Users/ Accounts specified
United of States	6,231	93%	12,243
India	2,027	66%	3,427
Brazil	1,615	90%	2,222
United Kingdom	1,455	64%	1,764
Germany	1,426	45%	2,027
France	1,404	44%	1,779
Italy	844	51%	1,124
Australia	444	65%	496
Republic of Korea	257	37%	393
Japan	90	59%	117

Source: www.google.com LI YI / CHINA DAILY

The US topped a list released by Twitter that detailed data and takedown requests from governments to the social media giant.

The "transparency report" showed the US made 679 requests relating to 948 users or accounts in the first half of 2012. Twitter had met 75 percent of the country's requests.

The micro-blogging site said all countries made fewer than 12 requests for user information in the first half of 2012, except Japan and the US.

The US also topped a similar transparency report from search engine Google, with 6,321 requests to remove content in the second half of 2011. The company granted the US 93 percent of their requests.

In Australia, the Labor government has been pushing for unprecedented powers to intercept all Internet communications.

Under the proposals, everything Australians do online, from Skype calls to Twitter and Facebook posts, would be stored for six to 24 months so security agencies can explore the data.

Australian residents are already subjected to intensive monitoring of their telecommunications, with intelligence and law enforcement agencies granted nearly a quarter of a million data intercept requests under the existing legislation in 2010 and 2011, according to Australian official data.

In the United Kingdom, a country which experienced Web initiated riots last year, the government published details of new cybersecurity plans in April, that included ordering ISPs and phone networks to store user data and make it available to security services.

> **We Americans seem to believe in a double standard ... but at the same time we'll scream bloody murder if any foreign government gets access to the data of US citizens or our government."**
>
> CHRIS SOGHOIAN
> GRADUATE FELLOW AT THE CENTER FOR APPLIED CYBERSECURITY RESEARCH AT THE UNIVERSITY OF INDIANA

According to UK media, the databases would record the phone numbers and email addresses of senders and receivers, chat messages sent within videogames, direct messages on Twitter, and private messages on Facebook.

To cope with such a massive surveillance project, UK officials unveiled a plan to invest more than $1 billion to improve national cybersecurity.

BBC Channel 4 News quoted Chris Soghoian, graduate fellow at the Center for Applied Cybersecurity Research at the University of Indiana, saying the law would be difficult to operate effectively without the cooperation of the United States, the home of many of the social media and email companies which would be the target of surveillance.

"Consumers are increasingly using services which are based outside the UK, often American companies that have no UK presence. As such, without the assistance of the US government, this proposed wiretapping law is simply not going to be effective," Soghoian said.

"We Americans seem to believe in a double standard — our government wants unfettered access to the private data of everyone else in the world, but at the same time we'll scream bloody murder if any foreign government gets access to the data of US citizens or our government.

"To be honest, as long as everyone in the world relies on services provided by American Internet companies, this double standard will continue."

Analysts said these proposed new measures to allow governments to see online data is the greatest expansion of the powers of security institutions since the Internet proved it can be a major force in social turmoil.

Western countries have realized that online freedom will threaten their domestic stability, said Su Hao, an expert on global affairs with China Foreign Affairs University.

Western countries have seen that Internet freedom is a two-edged sword, which can deepen social problems, Su said.

People in Spain, Greece and France organized mass demonstrations through social networks, beyond the governments' expectation.

In the UK, social networks including Facebook and Twitter offered good communication channels during the London riots in August 2011.

It was after the riots that the UK government considered banning people from major social networks if they were suspected of inciting violence online.

"As soon as our own Western-style stability of the state is called into question, then freedom of expression is expendable," John Kampfner, chief executive of Index on Censorship, said at a major cyberspace conference in London.

"There should be one rule for all, including western governments."

According to Google's report, the UK made 1,455 requests to remove content from July to December 2011, with 64 percent granted by the company.

In the US, people also used social networks, including Twitter, to communicate during the Occupy Wall Street movement, a protest mainly against social and economic inequality that began in September 2011.

A report in the New York Times on July 9 said US government bodies, including federal, state and local law enforcement agencies and courts, made at least 1.3 million demands for subscriber information in 2011.

Su said social media websites that are easy to use, and can send messages to large numbers of people within seconds, can be used by criminals in ways that can affect a government's ability to rule.

Tang Lan, an expert on information security from the China Institute of Contemporary International Relations, said that while in the past Internet and telecommunication censorship in Western countries was relatively low, tighter controls have been imposed in recent years as the West begins to see the Internet as becoming too influential.

Western governments have attempted to become more involved in safeguarding information security in major privately owned companies, such as power plants, because if their security was compromised it can affect public safety.

Despite governments and experts on cyber monitoring claiming they need tougher controls for security reasons, the public has expressed concerns that governments spying on Internet and telecommunication systems may harm privacy and abuse their power.

Australian senator Scott Ludlam, communications spokesman of the Greens party, was quoted by the World Socialist website saying the latest proposals for censorship would erode privacy and "the very freedoms that our security agencies were intended to protect".

Ludlam told media it was critical for the parliamentary committee to ensure that someone was "watching the watchers". He called for a healthy balance to be struck between privacy concerns and genuine security.

Greg Nojeim, a senior counsel at the US-based Center for Democracy and Technology, told media that the new cybersecurity act allows too much personal information to be shared and used for reasons unrelated to cybersecurity.