



## SOPHOS SECURITY THREAT REPORT REVEALS ATTITUDES TO CYBERWARFARE

IT security and data protection firm Sophos has today published the mid-year 2010 Security Threat Report, revealing the findings of a survey\* into attitudes towards cyberwarfare and detailing other trends and developments in IT security for the first half of 2010.

Sophos's worldwide survey of 1077 computer users uncovers some alarming attitudes towards international cyber-espionage. Respondents were asked questions including whether they thought spying via hacking or malware attacks is an acceptable practice and if the computer networks of private companies in other countries are legitimate targets.

Some of the key findings of the survey indicate a relaxed attitude to state-sponsored cybercrime:

\* 63% of those polled believe that it is acceptable for their country to spy on other nations by hacking or installing malware (23% said yes at any time, 40% said only during wartime, 37% said no)

\* A staggering 1 in 14 respondents believe that crippling denial of service attacks against another country's communication or financial websites are acceptable during peacetime (49% said only in wartime, 44% said never)

\* 32% believe that countries should be allowed to plant malware and hack into private foreign

companies in order to spy for economic advantage (23% said this was only acceptable in wartime, 9% said in peacetime, 68% said no)

"It's perhaps surprising that so many people seem to think that using the internet as a tool for spying, or even as a weapon, is acceptable practice," said Graham Cluley, senior technology consultant at Sophos. "After all, by giving the green light to these kind of activities you'd also have to expect to be on the receiving end too. Maybe yours will be the next company probed by an overseas power?"

'Operation Aurora', which first came to light at the start of the year, resulted in Google accusing Chinese hackers of cyberwarfare, as its systems, and those of other companies, were hit with targeted attacks, potentially signalling the most obvious sign yet of a new age of malware.

"Hacking and virus-writing began as a hobbyist activity, often designed to prove how smart the programmer was, rather than to cause serious long-term harm," continued Cluley. "It evolved into organised criminal activity, with the lure of large amounts of money and now, in 2010, it could be argued that the third motivation is using malware and the internet to gain commercial, political and military advantage over others."

A journalist-specific edition of the full Mid-year 2010 Security Threat Report, which contains further findings from the survey can be downloaded by journalists here (no registration required): <http://www.sophos.com/trmy10>

\*Sophos online survey, 1077 respondents.

About Sophos

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing security and data protection solutions that are simple to manage, deploy and use and that deliver the industry's lowest total cost of ownership. Sophos offers award-winning encryption, endpoint security, web, email, and network access control solutions backed by SophosLabs - a global network of threat intelligence centers. With more than two decades of experience, Sophos is regarded as a leader in security and data protection by top analyst firms and has received many industry awards.

Sophos is headquartered in Boston, US and Oxford, UK.

More information is available at [www.sophos.com](http://www.sophos.com).

Sophos Plc, The Pentagon, Abingdon Science Park,  
Abingdon, OX14 3YP, United Kingdom.

Company Reg No 2096520. VAT Reg No GB 348 3873 20.