

O.H.M.S.S

ON HER MAJESTY'S SECURITY STRATEGY



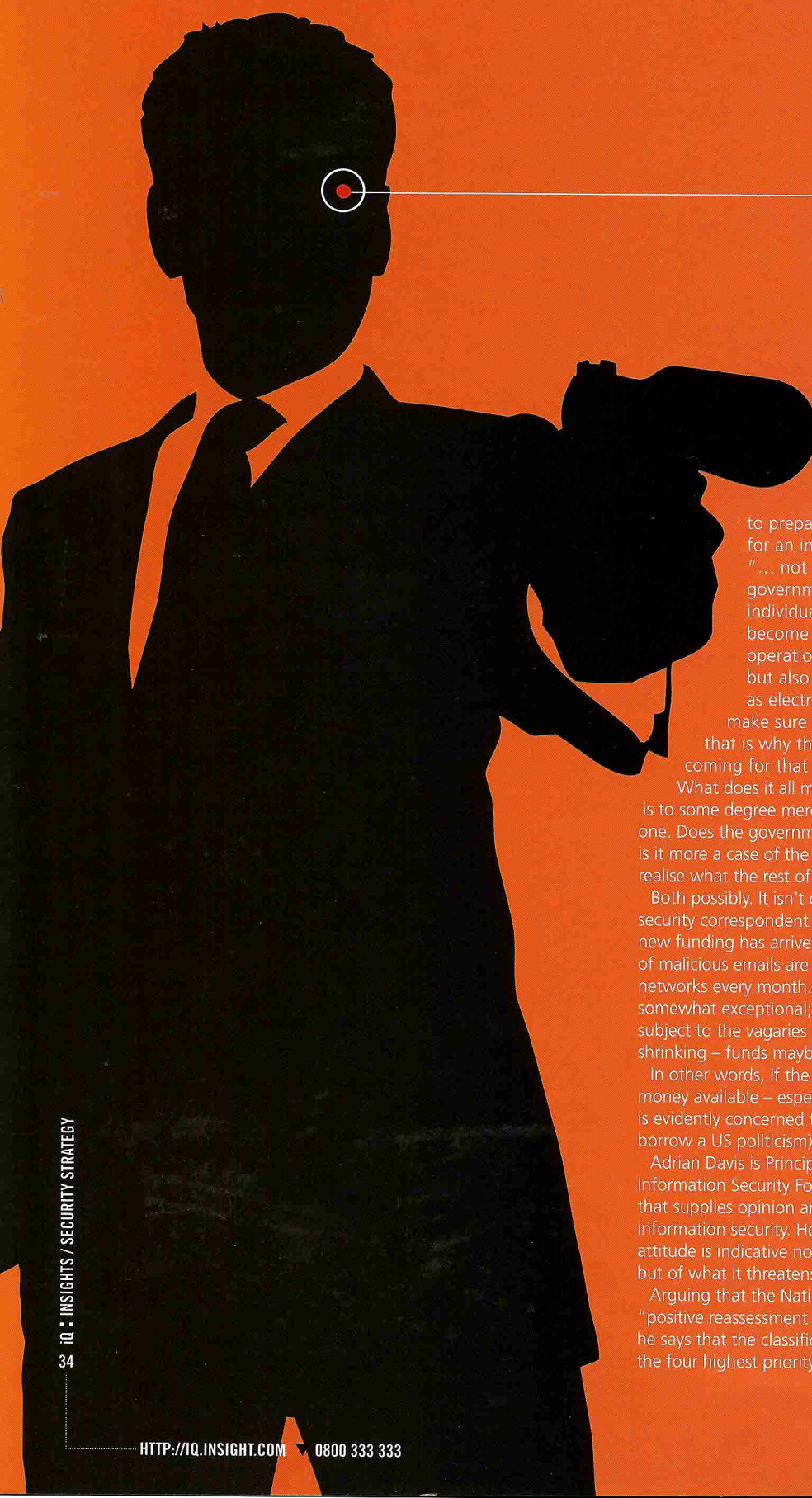
With the Government's recently unveiled National Security Strategy making special reference to the growing threat now facing Britain from cyberspace, IT security may finally be winning the official recognition and credence it merits, writes Harriet Knox.

I'm not sure if you've heard anything about it at all, but apparently the government has been announcing all sorts of public spending cuts and tax hikes lately. Something about a global financial crisis of frightening proportions forcing us into enormous and unprecedented levels of debt. OK. Whatever.

At any rate, with Gorgeous George and Co. tightening the purse strings and paring expenditure down to an absolute minimum, it looks as though things are going to be a bit tight for a while. Which is why we were perhaps just a tad surprised to hear that, following the National Security Council's recent announcement of the new National Security Strategy (and hot on the heels of the government's much-vaunted and debated Spending Review), an extra £500m has been earmarked to bolster cyber security. Is the government at last getting truly strategically serious about tech security then? Apparently.

Coming in the wake of another report (this one into the specific dangers of cyber crime, terrorism, and warfare), itself unveiled ahead of the Review, the news drew supporting comment from both Home Secretary Theresa May, and her counterpart in the Foreign Office, William Hague.

Comparing online crime with international terrorism, May admitted that attacks on computer networks are now among the biggest emerging threats to the UK. The Foreign Secretary meanwhile, who spoke about focusing on the protection of key infrastructure and defence assets, said →



that unless addressed it (cyber terrorism) could threaten the UK's economic welfare.

Noting the new strategy's specification of the threats for which the UK "most has

to prepare", Mr Hague backed the need for an increased protection capability:

"... not only against cyber attacks on the government, but on businesses and on individuals. Such attacks can, in the future, become a major threat to our economic operations... and our economic welfare, but also to national infrastructure, such as electricity grids and so on. We have to make sure we are protecting ourselves and that is why there is £500m of additional funding coming for that area."

What does it all mean though? If, as some suggest, it is to some degree merely a gesture, it is certainly a pricey one. Does the government know something we don't? Or is it more a case of the powers that be finally coming to realise what the rest of us have known for ages?

Both possibly. It isn't clear. But, perhaps tellingly, BBC security correspondent Frank Gardner notes that the new funding has arrived amid evidence that hundreds of malicious emails are now being aimed at government networks every month. The move is also, he hints, somewhat exceptional; defence reviews usually being subject to the vagaries of what limited – and perhaps even shrinking – funds maybe available.

In other words, if the government is making entirely new money available – especially at a time of such austerity – it is evidently concerned that the threat must represent (to borrow a US politicism) a clear and present danger.

Adrian Davis is Principal Research Analyst at the Information Security Forum (ISF), a not-for-profit body that supplies opinion and guidance on all aspects of information security. He believes the UK regime's new attitude is indicative not just of the threat from cyberspace, but of what it threatens.

Arguing that the National Security Strategy marks a "positive reassessment of the threats of the 21st Century", he says that the classification of cyber attack as one of the four highest priority risks facing the UK for the next

five years is "a recognition of the UK's dependence on the electronic sectors of the economy."

As part of his organisation's Threat Horizon programme, cyber crime has featured for some time as a threat for which the ISF's Member organisations (large corporates and governments around the world) have been advised to prepare. Moreover, says Davis, with increasing business dependence on critical infrastructure such as the Internet, the potential for criminal attacks to morph into terrorist or state sponsored cyber attacks with the potential for catastrophic impact is a serious and growing threat.

Others however, including GFI Software's Senior Threat Researcher, Christopher Boyd, seem less convinced about the governments' underlying motives. He suggests that, particularly in view of their timing (i.e. immediately ahead of a major spending review), these increased warnings about 'cyber terror' smack of an attempt to secure funding and avoid cuts.

"The UK Government warns that this is a grave threat, yet continues to use Internet Explorer 6; a browser that has been largely discredited due to its numerous security flaws!" he comments.

His concern, then, is clearly that the measures don't go far enough. "As a country, we have struggled to deal with modest, home-grown threats effectively – such as those posed by script kiddies – so what chance do we have against professional computer criminals with our current grass roots law enforcement, intelligence and counter terrorism capabilities and initiatives?"

"Until recently, you couldn't even report computer crime to the National Hi-Tech Crime Unit (NHTCU) – you had to go to a local police station and hope the officer at the desk knew what you were talking about and escalated your report to the right department."

As such, argues Boyd, money isn't enough. There must also be a commitment to deploying the right technologies and expertise. "In order to effectively respond to growing cyber security threats – regardless of whether they are perceived or proven – it is essential to invest in proven technologies to identify and repel external data threats", he says. The right people too. "People with the knowledge and expertise to anticipate and identify threats, and take appropriate action to secure key infrastructure, core networks, and devices at either a national or local level."

Perhaps more conciliatory, Davis says that the £500 ↵

**UNTIL RECENTLY, YOU
COULDN'T EVEN REPORT
COMPUTER CRIME TO
THE NATIONAL HI-TECH
CRIME UNIT (NHTCU) –
YOU HAD TO GO TO A
LOCAL POLICE STATION
AND HOPE THE
OFFICER AT THE DESK
KNEW WHAT YOU
WERE TALKING ABOUT.**

