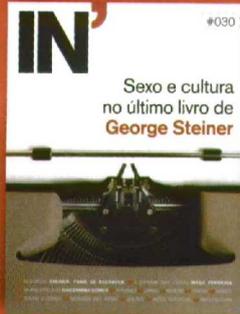


Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21

notícias sábado' 134

N S



#030
Sexo e cultura
no último livro de
George Steiner

+ Suplemento IN'

O percurso
de um judeu errante

Visita guiada ao mundo
literário de George Steiner

2 AGOSTO 2008 | SEMANAL | ESTA REVISTA FAZ PARTE INTEGRANTE DO DIÁRIO DE NOTÍCIAS Nº. 50883 E DO JORNAL DE NOTÍCIAS Nº. 53/121 | NÃO PODE SER VENDIDA SEPARADAMENTE



O regresso das casas de penhores

O negócio dos empréstimos sobre ouro, prata e jóias vai de vento em popa, depois de ter estado quase à beira da extinção. Acossados pela crise, cada vez mais portugueses vão pôr os objectos de valor no "prego"

ENTREVISTA A PAULO SOUSA
PRÉMIO IBM DE CIÊNCIA
"O ciberterrorismo é
uma ameaça muito real"

REGATA BREITLING
A Fórmula 1
da vela



CAÇADORES DE NAZIS
NA PISTA DE FUGITIVOS
Parecem avozinhos simpáticos
mas são assassinos sanguinários

Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21

18' Entrevista

PAULO SOUSA

É preciso garantir a segurança contra o ciberterrorismo

[Terminal]

Perfil

Paulo Jorge Sousa, 29 anos, é professor auxiliar convidado no departamento de Informática da Faculdade de Ciências da Universidade de Lisboa. Por pouco a vida não lhe pregou uma rasteira no secundário, quando as dificuldades financeiras da sua numerosa família quase o fizeram trocar os estudos por um emprego. Mas os professores estavam atentos, conheciam-lhe o génio e a força de vontade e incentivaram-no a continuar, com o apoio de bolsas de estudo. Na faculdade onde estudou (e agora ensina e investiga), foi o melhor aluno de 1999-2000 e o melhor recém-licenciado em Informática no ano seguinte, finalizando a licenciatura com 18 valores e 19 na sua área específica. No doutoramento em Informática foi aprovado por unanimidade também com 19 valores. Desde então, participa em diversos projectos e redes de excelência financiados pela Comissão Europeia e pela Fundação para a Ciência e Tecnologia. Além de colaborar com diversas publicações especializadas no País e no estrangeiro, Paulo Sousa integra o LaSIGE (Large-Scale Informatics Systems Laboratory) e pertence ao grupo de investigação Navigators.

Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21

Todas as empresas que operam infra-estruturas indispensáveis para o funcionamento da sociedade – como a rede de distribuição de electricidade, água ou telecomunicações – usam a Internet e, desse modo, sujeitam-se ao ataque de piratas informáticos desejosos de provocar danos no tecido social. Paulo Sousa, 29 anos, professor de Informática e investigador da Faculdade de Ciências da Universidade de Lisboa, descobriu um método pioneiro de defesa automática dos mecanismos de protecção, a que deu o nome de “resiliência proactiva”. “É como se os piratas tentassem abrir feridas num corpo e ele se recompusesse continuamente”, explicou à **NS’**

TEXTO ANA PAGO FOTOGRAFIA JOÃO GIRÃO

Ganhou o Prémio Científico IBM 2007 pelo seu trabalho sobre a segurança dos sistemas de informação. Como foi isso?

Só iniciei o trabalho na área da segurança no início do meu doutoramento, antes disso fiz alguma investigação, durante dois anos, mas sempre na área de tempo real, carros que se autoconduzem... No doutoramento, o professor Paulo Veríssimo propôs-me realizar um trabalho e eu aceitei o desafio. E na altura, talvez por falta de maturidade, eu até nem achava que houvesse muito trabalho a desenvolver em segurança. Mas a verdade é que existem imensos problemas.

As infra-estruturas que permitem o funcionamento da nossa sociedade estão sob ameaça?

Sim, sim, sem dúvida. Não só infra-estruturas eléctricas, mas também as das telecomunicações, da água ou do gás, porque todas usam sistemas informáticos e hoje em dia eles estão interligados pela Net. Os operadores que controlam esses sistemas têm um computador e estão na empresa a supervisionar e a aceder à rede ao mesmo tempo. E embora as empresas digam “Não, não usamos computadores diferentes para aceder à Web e para controlar”, não

é verdade. Auditorias recentes mostraram que essas empresas, basicamente, têm dois cabos de rede ligados ao computador: um a controlar o equipamento e outro a controlar a Net. Um pirata que saiba isto pode comprometer o computador do operador e, daí, saltar para dentro da infra-estrutura e dar cabo de tudo.

Na apresentação do seu sistema de protecção falava de apagões frequentes nos EUA e na Europa, normalmente atribuídos a tempestades. É mesmo assim?

Oficialmente, na maioria dos casos, sim. Embora em relação ao apagão de 2003, ocorrido no Nordeste dos EUA e do Canadá, e que durou cerca de nove horas, haja hoje rumores (vários jornais *online* libertaram a notícia) de que poderá ter sido provocado por cibercriminosos chineses. Existe essa desconfiança, apesar de nunca ter havido nenhuma confirmação oficial. E a maior parte dos apagões deve-se

realmente a acidentes. Mas se os estragos assim já são grandes, quando for a sério e malicioso, será muito pior.

Referiu uma experiência em que os investigadores conseguiram rebentar com um gerador, via Internet. Isso significa que a ameaça é real...

Muito real. A CNN fez uma reportagem que mostra isso mesmo, com pessoas importantes da CIA a confirmarem que é uma ameaça, que aprenderam muito com a experiência e que conseguiram fortalecer a segurança dos sistemas, embora saibam perfeitamente que não estão seguros. Nenhum sistema pode garantir, tal como nós não podemos garantir com a nossa solução, que um pirata não entre. Estamos é a diminuir cada vez mais as probabilidades de alguém entrar.

Existem ataques que não chegam ao conhecimento público?

Sim, com toda a certeza, e muitos deles em sistemas críticos, como a banca. Obviamente que não se vai alarmar a população dizendo que um pirata provocou um apagão, dado que isso ia gerar insegurança. Ainda na cerimónia de entrega do prémio, o ministro da Ciência [Mariano Gago] mencionou um estudo que diz

“O ministro Mariano Gago mencionou um estudo que diz que a solução perfeita para evitar ataques seria desligar a Internet; eu compreendo: o papel dele é acalmar as pessoas”

Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21

que a solução perfeita para evitar ataques seria desligar a Internet, e eu compreendo: o papel dele é acalmar as pessoas. Não podia simplesmente dizer que concorda comigo, quando sugiro que tudo pode estar em risco. **Desligar a Internet seria impossível nos dias que correm, não?**

Obviamente. Essa nunca seria uma solução viável. Havia pessoas da EDP na audiência, atentas, e elas próprias me confirmaram que não era solução.

Que repercussões poderia ter um atentado contra uma infra-estrutura de distribuição de energia eléctrica?

Um apagão que poderia demorar semanas,

talvez meses. Ao fim de algumas horas, iria comprometer a iluminação eléctrica, as televisões, computadores, multibancos e bombas de combustível. Ao fim de alguns dias deixávamos de ter também transportes, comida nas lojas e geradores de emergência nos hospitais. **Seria o caos total...**

Claro! Um ataque deste género destruiria equipamento, e este não só demora muito tempo a repor (um gerador pesa algumas toneladas), como depois o processo de reinício tem de ser algo muito controlado, a fazer-se gradualmente, porque o modo como a rede eléctrica funciona é outro problema: tem de estar tudo bem estabilizado, senão rebenta. E nessas nove horas de apagão de que eu falava há pouco foi isso mesmo que aconteceu: demorou tudo imenso tempo a religar, nem sequer foi a substituir. Supondo que os componentes arderam e vão ter de ser substituídos, a situação leva ainda mais tempo a regularizar.

Em última análise, poderia conduzir a uma catástrofe...

O mais possível! É uma ameaça real. E por isso existem vários projectos de investigação, dos quais o principal na Europa é o Crutial, em que estamos envolvidos. Ainda há pouco tempo houve um encontro nos EUA e convidaram o professor Paulo Veríssimo, aqui do LaSIGE [Laboratório de Sistemas Informáticos de Larga Escala da Faculdade de Ciências], para fazer uma apresentação. Ele mostrou os resultados do nosso projecto e foram muito bem aceites. O tema é muitíssimo actual.

Até que ponto os nossos sistemas de distribuição de energia eléctrica são sensíveis?

São muito sensíveis, em Portugal e no mundo, porque a sensibilidade reside fundamentalmente no sistema informático, e o que controla esses sistemas de rede eléctrica são computa-

Uma questão de “resiliência”

E se, de repente, um ciberterrorista lançasse um ataque contra o processo de monitorização de um centro de controlo de uma subestação de energia eléctrica? O atacante procurava descobrir uma vulnerabilidade na *firewall* (protecção do sistema informático) para assumir o controlo das operações. Azar do pirata, caso o centro de controlo estivesse atento ao trabalho de Paulo Sousa e tivesse mandado instalar a *firewall* com resiliência proactiva. A protecção seria tolerante a intrusões e as réplicas regeneradas periodicamente, o que obrigaria o adversário a ter de bater recordes de velocidade e inteligência para capturar duas réplicas entre regenerações em apenas sete minutos e meio.

Ao contrário do que se passava com as protecções clássicas, explica Paulo Sousa, “com a resiliência proactiva, o *hacker* tem apenas minutos, e não dias, para fazer o ataque”. Num sistema real, já seria muito difícil para o pirata conseguir atacar duas réplicas em pouco tempo. “Aqui, mesmo que ele ataque uma segunda réplica, não lhe vai servir de nada porque, entretanto, a primeira danificada já se regenerou”, traduz o investigador, sublinhando o facto de todas elas serem diferentes umas das outras e regeneradas a um nível externo ao sistema, de modo a dificultar boicotes. Nunca os ciberterroristas tiveram tantas dores de cabeça a tentar “furar” a ciência...

Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21

dores que podem ser comprometidos exactamente da mesma forma que os computadores de casa. A diferença é que nas máquinas de controlo esse comprometimento vai resultar na desestabilização de um processo físico (o de produção da energia eléctrica), e isso tem impacto na sociedade.

Um ataque assim pode ser considerado uma forma de ciberterrorismo?

É ciberterrorismo, sim. O nome certo é mesmo esse, o conceito aplica-se a esse tipo de ataques. Já houve no passado intrusões em sistemas *online*, como o da banca electrónica, mas aí não

“Um atentado contra uma infra-estrutura de distribuição de energia eléctrica provocaria um apagão que poderia demorar semanas, talvez meses”

Tivemos outros sucessos no passado, como o projecto Maftia, com o qual fomos à final do Prémio Descartes.

E ganharam?

Venceu a cura para um cancro, o que percebemos perfeitamente. Mas estivemos na final. Foi a primeira vez que um projecto de informática chegou à final daquele prémio europeu de investigação, e nós estivemos lá com o trabalho do Maftia, em que se desenvolveu a tal tolerância a intrusões que valeu ao professor Nuno Neves o Prémio IBM 2004. E este Crutial, no fundo, aplica as ideias do Maftia à infra-

estrutura eléctrica, juntando-lhe a resiliência proactiva que regenera os sistemas informáticos. É uma das grandes conquistas do Crutial a partir da investigação portuguesa.

Quanto tempo demorou a desenvolver o sistema de protecção que ganhou o prémio?

A *firewall* começou a ser criada há cerca de dois anos e ainda está a ser desenvolvida, continuamos a melhorá-la. Mas não foi a *firewall* propriamente dita que mereceu este prémio: ele foi atribuído à propriedade regeneradora da resiliência proactiva, que por sua vez foi aplicada à protecção. Começámos por desenvolver uma primeira *firewall* tolerante a intrusões, do professor Nuno Neves, que recebeu o Prémio Científico IBM em 2004. E esta que usa agora as minhas ideias, a mais forte de todas, só foi possível porque ganhou as caracte-

terísticas da anterior.

O que quer dizer “resiliência proactiva”?

Quer dizer que, se acontecer um determinado número de intrusões durante o seu funcionamento, a *firewall* continua a funcionar bem. E, como tem aquela capacidade nova de regeneração, não fica limitada a poder combater apenas uma ou duas intrusões: podem ser intrusões ilimitadas, que ela dá conta do recado. Regenerar é a palavra de ordem deste projecto desenvolvido por mim e por mais um grupo de colegas, nomeadamente o professor Nuno Neves, o professor Paulo Veríssimo, Alysson Bessani e Paulo Correia. A *firewall* é dos cinco. **Portugal está ao nível dos melhores do mundo em termos de investigação científica?**

Sem dúvida. O único projecto que se está a debruçar sobre este tema na Europa é o Crutial, e nós estamos lá, fomos convidados a integrá-lo.

estrutura eléctrica, juntando-lhe a resiliência proactiva que regenera os sistemas informáticos. É uma das grandes conquistas do Crutial a partir da investigação portuguesa.

Quais são os maiores obstáculos que enfrenta no trabalho de investigação?

A falta de fundos é o mais gritante. Temos tido sorte, na medida em que vamos sempre conseguindo participar em projectos e, desde que estejamos dentro de pelo menos um projecto europeu, temos dinheiro para contratar alunos de doutoramento, que são fundamentais, porque é esse pessoal mais novo que faz a máquina avançar. O problema é que é muito complicado ganhar um projecto europeu. Neste momento, estamos em dois e numa rede de excelência, mas são projectos de três anos, que quando acabam fazem-nos andar ali num período negro. E vai havendo algum financia-

mento para o LaSIGE, mas insuficiente para manter a investigação de ponta que desenvolvemos.

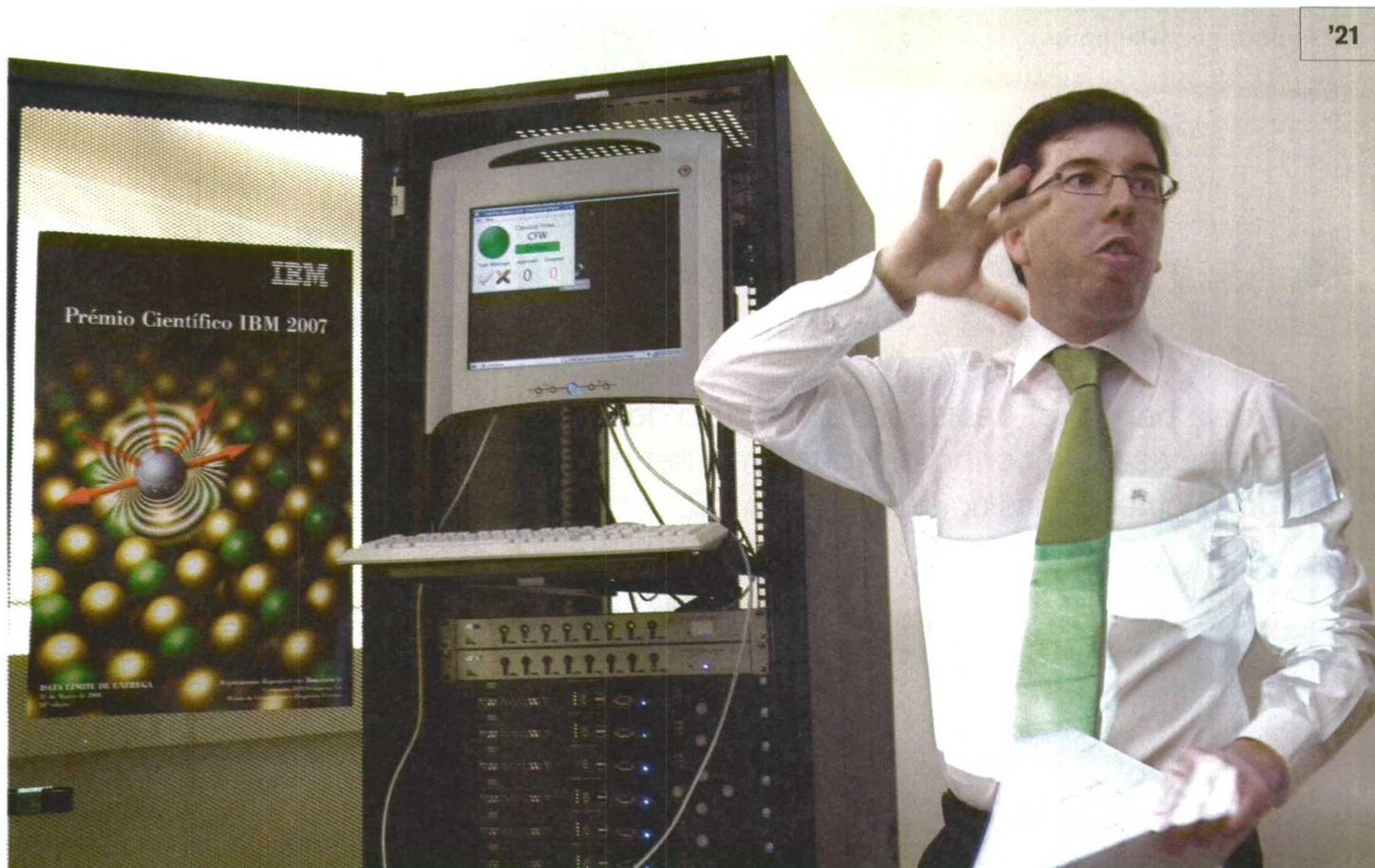
Qual é então o caminho a seguir?

As opiniões divergem sobre esse assunto. Pessoalmente, acho que deviam premiar-se os laboratórios pelos resultados que obtêm – no caso do LaSIGE, tem conseguido resultados brutais nos últimos anos: venceu duas vezes o Prémio IBM, fomos à final do Prémio Descartes, temos vários projectos europeus que demonstram que este é um laboratório de excelência, que devia receber fundos todos os anos. Se já fez e continua a fazer tanto, é sinal de que temos cá as pessoas certas para produzir.

Mas não é assim que o Ministério da Ciência avalia?

Não, o ministério financia sobretudo laboratórios associados, que não estão ligados a univer-

Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21



sidades e supostamente reúnem a nata dos investigadores, é dali que se esperam os grandes resultados. Estes laboratórios mais pequenos, ligados a uma determinada faculdade, não são bem-vistos hoje em dia.

O que sentiu ao receber este prémio?

Foi muito importante, não só porque coroo o meu trabalho, como o do laboratório e o de todo o departamento de informática da Faculdade de Ciências da Universidade de Lisboa. Tem um significado muito forte, é o melhor prémio da área em Portugal e não sei quais serão todas as consequências que terá, mas estou radiante. Quando o presidente da IBM me telefonou a anunciar que tinha ganho nem coube em mim. Ele até comentou comigo que já não via uma reacção assim há uns tempos, porque normalmente é pessoal mais velho – e mais comedido – que recebe esta distinção.

Quais são as qualidades que definem um bom investigador?

Primeiro tem de gostar daquilo que faz, ter

de forçar todos os dias não resulta em nada de jeito no caso da investigação. Depois tem de trabalhar muito, ter brio, dar sempre o melhor e ter sorte. (*Risos*) O júri podia ter-se decidido por outro trabalho, mesmo que não fosse melhor. A sorte aqui não é mesmo a variável menos importante, por mais que trabalhemos para ela.

O departamento de informática da Faculdade de Ciências é o melhor lugar para se trabalhar? Em Portugal sim, sem sombra de dúvida. Este

laboratório é o laboratório, não vejo melhor sítio. Já tive outros convites, inclusive do Instituto Superior Técnico, para a mesma área, e não fui. E eles são muito fortes noutras vertentes que não esta da segurança informática, se calhar lá até ia ter mais espaço de manobra, porque

ainda está tudo bastante incipiente... Mas tive de recusar o convite, este é o meu sítio.

Considera a possibilidade de ir trabalhar para o estrangeiro?

Não está nos meus planos ir para o estrangeiro. Gosto muito de Portugal e, além disso, sinto que seria uma espécie de traição sair. Aqui recebi muitas bolsas de estudo desde o 10.º ano, incluindo uma da Gulbenkian, e desde o primeiro ano da faculdade que sempre consegui outras que me ajudaram. Não tive nenhuma no doutoramento, mas mesmo aí fui apoiado com dinheiros do Estado. E tendo havido esse esforço, vou dar o retorno.

Quais são os projectos que se seguem?

Gosto muito da área da segurança informática, quero continuar com ela. Se um dia saísse da faculdade seria para abrir uma empresa nesta área, não existem muitas. Aqui, agora, estamos para já a pensar aplicar os resultados do projecto Crutial na protecção de outras infra-estrutu-

Diário Notícias notícias sábado 02-08-2008	Periodicidade:	Diário	Temática:	Tecnologia
	Classe:	Informação Geral	Dimensão:	1425 cm²
	Âmbito:	Nacional	Imagem:	S/Cor
	Tiragem:	79040	Página (s):	1/18 a 21

“A sensibilidade reside no sistema informático e o que controla esses sistemas de rede eléctrica são computadores que podem ser comprometidos por ciberterroristas”

ras críticas, como as telecomunicações (se ficarmos sem elas também é o caos!), a água e o gás.

Como é que a sua família lida com esta paixão pela informática?

A dedicação à investigação dura dia e noite, é impossível não estarmos sempre a pensar, a plane-

ar as aulas, a relacionar o trabalho com pormenores de um filme que vemos em casa... é assim que uma pessoa avança. Mas também é verdade que gostava de ter muito mais tempo do que tenho para a minha mulher e os meus três filhos.

Eles convivem bem com o seu trabalho?

A minha mulher também trabalha em informática e entende, mas tento não levar muito trabalho para casa, embora seja inevitável.

E depois os miúdos (tirando o bebé) também gostam e acabam por conviver com a área: o meu filho mais velho, de sete anos, tem um grande gosto pela informática e é muito motivado por mim, pela mãe e pela escola. Depois, ele há-de escolher o que quiser, mas fico contente. E a Vitória, de quatro anos, também começa a ter algum contacto com os computadores, mas é menina e pequena. Ainda troca a informática pelo *ballet* e desconfio que vai continuar assim. ■