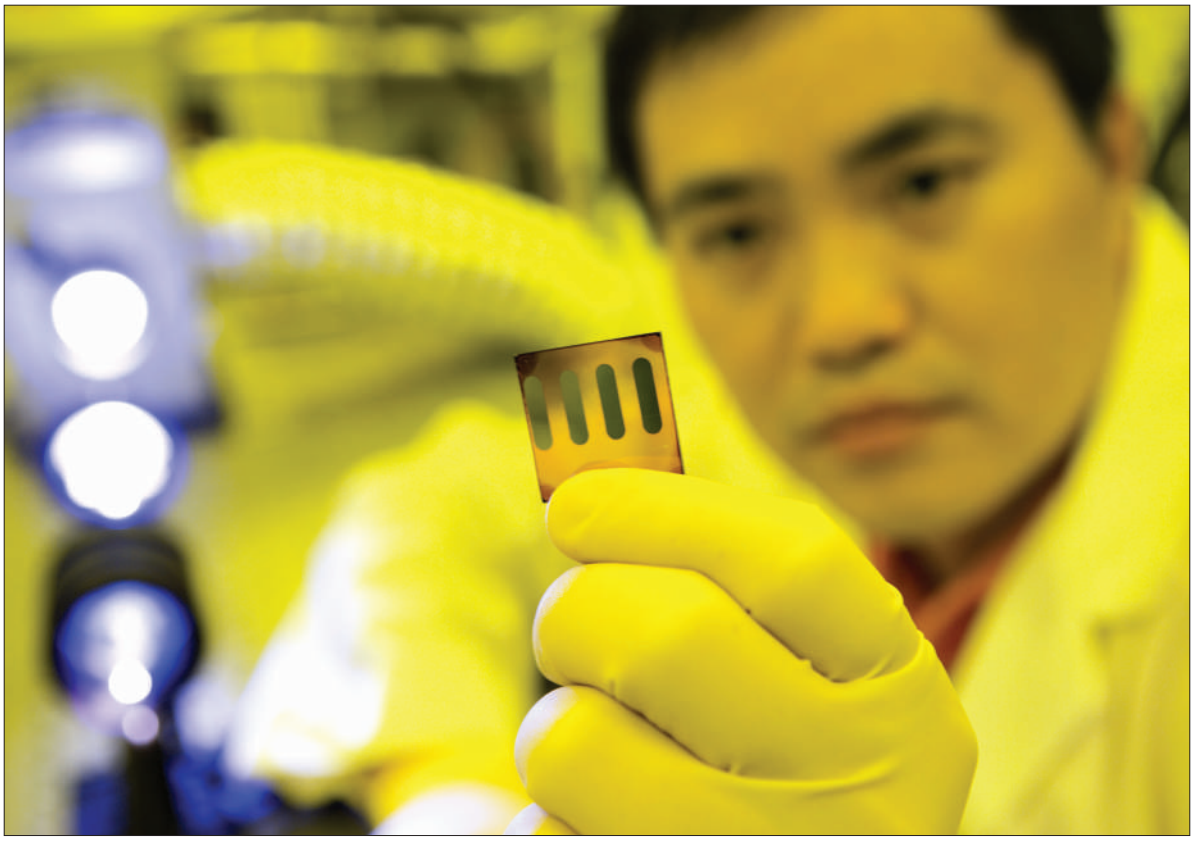

Singapore Journal of

Scientific Research

ISSN: 2010-006x

science alert

http://scialert.net/sjsr

Is Internet Backbone Vulnerable to Cyber Attack?

While cyber attacks on the internet involving malware, hacking and distributed denial of service are featured in the headlines most often, researchers in Switzerland suggest that physical attack on internet backbones, servers and internet data hubs could be just as important a problem in sustaining network functions.

Writing in the December issue of the International Journal of Critical Infrastructures, the team suggests that physical damage to critical communication networks can lead to a cascade of failures and major disruption to functions due to the interdependency of different critical infrastructures. In 2003, university student Sean Gorman famously mapped the paths of fibre-optic cables across the USA for his PhD dissertation at George Mason University and showed just how easy it would be to locate critical choke points from public records and data. It would not be difficult to block those choke points. Moreover, carriers under increasing economic pressure are not investing in redundant fibre-optic cables and are also simply using road and rail conduits to cut costs and avoid construction works across cities.

"All this brings critical communication backbones into a potentially unsafe condition," says Ling Zhou of the Laboratory for Safety Analysis, Swiss Federal Institute of Technology Zurich (ETH). She points out that fibre optic cables are not the only vulnerable components of the internet. Other physical components of the internet, like servers, bridges and hubs, routers, personal computers, can also be vulnerable parts.

"Effective functioning of today's societies is based on critical infrastructures, i.e., large scale infrastructures whose degradation, disruption or destruction would have a serious impact on health, safety, security or well-being of citizens or the effective functioning of governments and/or economy," However, most critical infrastructures are privately owned. The owners and operators focus on their own infrastructure and business framework and have only limited interest in the consequences of failed components beyond their domain.

The coincidence of two accidental physical problems in January 2006, knocked out internet access across the western USA. Internet traffic had been rerouted via Arizona after flood damage to equipment in California but construction workers accidentally cut through a fibre optic cable there knocking out Sprint's Western US network for three and a half hours on the afternoon of the 9th. Other similar incidents occur unpredictably, usually when two or more physical faults occur at the same time or coincide with virtual issues such as the spread of malicious software or traffic overflow. This one incident simply highlights just how vulnerable the networks could be to deliberate physical attacks at two or more places.

Zhou has used SWITCH, the Swiss national network for research and education, as the focus of a case study and simulation of how such physical damage might impact on networks and the internet as a whole in the future.

Her results offer three main recommendations for protecting critical network infrastructure that should be considered at the national level:

* First Common connection points, where several cables or network hubs meet, should be regarded as key protected infrastructure.
* Secondly, backbone and service providers should be persuaded and supported in protecting their network backbone and to diversify the physical routing of fibre optic cables.
* Thirdly, national governments need to cooperate with service providers and define a series of basic safety standards for what is currently an entirely unregulated sector of information and communication technologies.

Ling Zhou et al. Vulnerability analysis of the physical part of the internet. International Journal of Critical Infrastructures, 2010, 6, 402-420