Curry, J. and Austin, G. (2019) 'A cyber storm on the horizon', *ITNOW*, 61 (2), pp. 38-39.

A Cyber Storm on the Horizon

John Curry, Senior lecturer Games Development and Cyber security, Bath Spa University, UK.

Greg Austin, Professor Greg Austin, University of New South Wales, Canberra, Australia, UK

In November 2017, a major metropolitan local authority in the south west of the UK came under sustained cyber-attack. Phishing emails successfully installed malware; a denial of service attack was started at the same time and social media 'trolls' attempted to cause panic. The cause of the attack was nothing to do with the local authority; it was linked to British foreign policy in Syria.

The local authority staff were gradually faced with multiple applications on their desk tops, including their primary email being unavailable. The situation looked serious, but the local authority carried on. The attack failed. The reasons why the attack failed are worth noting.

- *Defence in depth due to fragmentary IT procurement*. The local authority procurement meant they used a wide variety of software, hardware, operating systems, plus staff switched to their own devices to carry on working.
- *Back up email system*. One email system was hit, but the authority had another legacy email system in place, with many managers having two email addresses (one for each system). Some staff used their private email to communicate.
- *Failure to target critical applications*. Then attackers did not really understand the business processes of their target. One of the systems affected was the invoicing system; however not being able to invoice for 24 hours had no real impact on cash flow of the organisation. The failure of the home care scheduling system had no effect, as the care workers were in a routine and knew where they should work, even without electronic prompting.
- *Servers had spare capacity.* The scale of the DDOS attack was not sufficient to significantly impact the targeted servers. The attackers had not fingerprinted these servers and accurately calculated the volume of attack necessary to success.
- *Speed of response.* The authority also acted with commendable speed; the emergency planning team delegated the response lead the IT staff. IT services immediately disrupted their normal operations and all staff were focussed on the attack. Consultants were called in within hours (but were not actually needed).
- *Social Media.* There was no social media storm to cause disruption within the city as key local well-known local social media 'stars' did not react.
- *National Media had no interest.* The national media ignored the attack, the story "local authority IT staff effectively mitigate cyber-attack" was perhaps not enticing enough headline.

Just two years ago, the concept of a cyber storm, a widespread disabling attack primarily through cyber, was rightly dismissed by policy makers responsible for essential services as being technically unfeasible. The cyber-attack on the British city outlined above was perhaps a window onto the future. Other cities have been subject to more effective cyber-attack recently. The best-known example, was the massive cyber-attack on the city of Atlanta in the USA in March 2018 using the SamSam ransomware. It was notable for the extent and duration of the services outage. The sustained chaos in Atlanta was caused by just two Iranian hackers, who had no identified affiliation with the Iranian state.

The growing feasibility of a cyber storm

Just a few years ago, the concept of a cyber Pearl harbour was not seen as credible by most observers. Now the idea of a cyber storm is not considered likely, but it can be seen as on the distant horizon as a possibility.

The IT is clearly one of the fastest, most innovate industries on the planet. The speed of change is accelerating, with the lead time from idea to implementation is continuing to shrink. The cumulative effect of these changes is making our cities more efficient (and sustainable), but also making them more vulnerable to cyber-attack.

One of key business drivers of technology has been the move towards homogeneity, with the laudable aim of efficient systems administration using integrated software management systems. One system, means one target and the impact of failure is critical. Another parallel trend has been to put services and data in the cloud, driving down costs, but this also creating a single point of failure if access to the cloud is interrupted.

A current issue that is the much-discussed rise of the Internet of things, linking huge number of devices via the Internet, offering tremendous advantages to society. These IoT devices have limited processing power, so stating the obvious, do not enjoy the level of security of the average computer. If compromised, the IoT will give the hackers access to a range of physical devices that will control our cities; from traffic lights, to water pumping stations.

The dark side of IT is mimicking the developments in the mainstream industry for its own purposes to enhance their capabilities. One trend has been the commodification of hacking tools. Off-the-shelf software malware that can be purchased, perhaps using Bitcoin, then rapidly customised as part of an attack. Hacking as a service has also emerged, with teams of hackers available to hire at short notice. The logical implication is that an attacker with a large enough budget can buy in hackers and attacks upon demand to scale up their efforts to disrupt their target.

Even more important has been the growth in the ability of the attackers to coordinate their attack using the same project management control tools as the rest of the industry. Going back into military history, the success of blitzkrieg on the battlefield was not new technology, it was the ability to coordinate all parts of an attack at once. The aim was to deliver a well-timed attack to overload resources of the defenders. Now it is feasible for hackers to buying in attack capacity to dynamically scale up their attack until successful.

Now the idea of a cyber storm is clearly on the distant horizon and developments in technology are moving it closer. Several leading states, including Britain, are actively planning to seed such a storm in foreign cities if war broke out or looked imminent. Bringing a modern city to a standstill by attacking the IT infrastructure is a really challenging task as any cyber wargame will demonstrate, and the next wave of attacks may not succeed. However, it is clear the hackers are certainly going to try.

Box out

In February 2019, experts from the UK, American, Canada, Israel, the Ukraine and other countries assembled at the University of New South Wales, Canberra, Australia to discuss and test the concept of a cyber storm. Major General Marcus Thompson, who leads the Australian Information Warfare Division, said “this was the scenario costing him sleep”.