THE CONVERSATION
Academic rigour, journalistic flair

lolloj

If two countries waged cyber war on each another, here's what to expect

August 5, 2016 11.01am BST

Imagine you woke up to discover a massive cyber attack on your country. All government data has been destroyed, taking out healthcare records, birth certificates, social care records and so much more. The transport system isn't working, traffic lights are blank, immigration is in chaos and all tax records have disappeared. The internet has been reduced to an error message and daily life as you know it has halted.

This might sound fanciful but don't be so sure. When countries declare war on one another in future, this sort of disaster might be the opportunity the enemy is looking for. The internet has brought us many great things but it has made us more vulnerable. Protecting against such futuristic violence is one of the key challenges of the 21st century.

Strategists know that the most fragile part of internet infrastructure is the energy supply. The starting point in serious cyber warfare may well be to trip the power stations which power the data centres involved with the core routing elements of the network.

Author

Bill Buchanan
Head, The Cyber Academy, Edinburgh Napier University

Back-up generators and uninterruptible power supplies might offer protection, but they don't always work and can potentially be hacked. In any case, backup power is usually designed to shut off after a few hours. That is enough time to correct a normal fault, but cyber attacks might require backup for days or even weeks.

William Cohen, the former US secretary of defence, recently predicted such a major outage would cause large-scale economic damage and civil unrest throughout a country. In a war situation, this could be enough to bring about defeat. Janet Napolitano, a former secretary at the US Department of Homeland Security, believes the American system is not well enough protected to avoid this.

William Cohen. Hasan Jamali

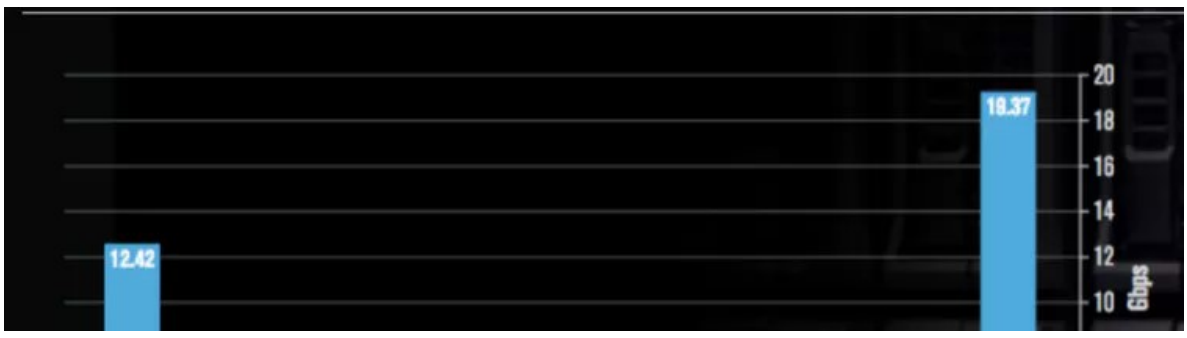
Denial of service

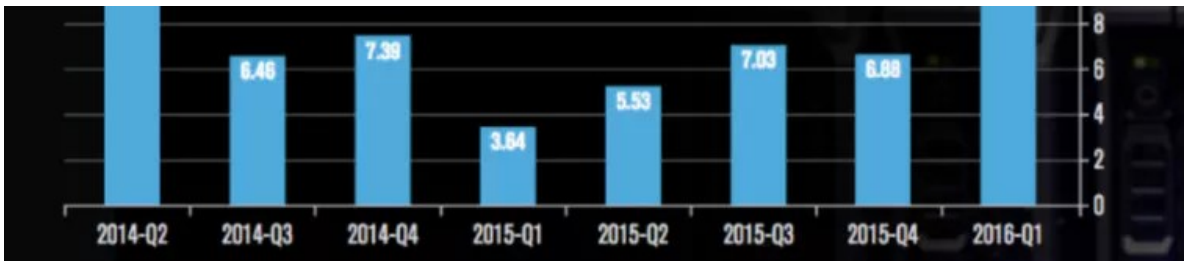
An attack on the national grid could involve what is called a distributed denial of service (DDoS) attack. These use multiple computers to flood a system with information from many sources at the same time. This could make it easier for hackers to neutralise the backup power and tripping the system.

DDoS attacks are also a major threat in their own right. They could overload the main network gateways of a country and cause major outages. Such attacks are commonplace against the private sector, particularly finance companies. Akamai Technologies, which controls 30% of internet traffic, recently said these are the most worrying kind of attack and becoming ever more sophisticated.

Akamai recently monitored a sustained attack against a media outlet of 363 gigabits per second (Gbps) – a scale which few companies, let alone a nation, could cope with for long. Networks specialist Verisign reports a shocking 111% increase in DDoS attacks per year, almost half of them over 10 Gbps in scale – much more powerful than previously. The top sources are Vietnam, Brazil and Colombia.

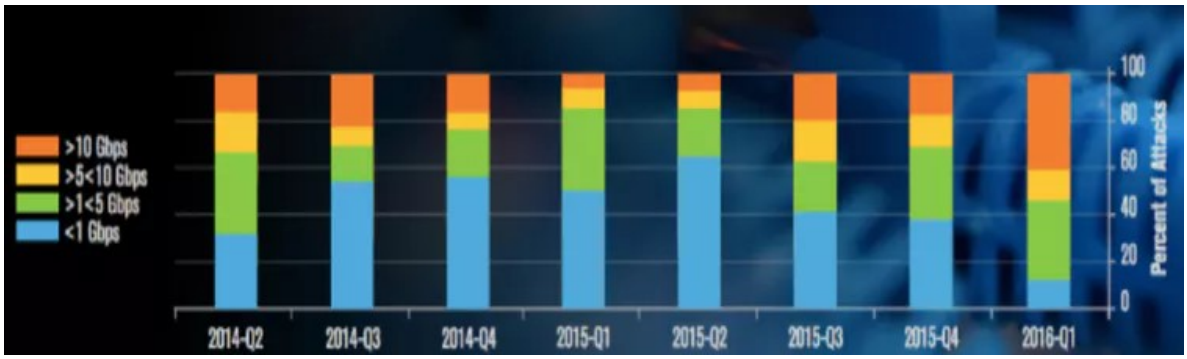
Number of attacks





Verisign

Scale of attacks



Verisign

Most DDoS attacks swamp an internal network with traffic via the DNS and NTP servers that provide most core services within the network. Without DNS the internet wouldn't work, but it is weak from a security point of view. Specialists have been trying to come up with a solution, but building security into these servers to recognise DDoS attacks appears to mean re-engineering the entire internet.

How to react

If a country's grid were taken down by an attack for any length of time, the ensuing chaos would potentially be enough to win a war outright. If instead its online infrastructure were substantially compromised by a DDoS attack, the response would probably go like this:

Phase one: Takeover of network: the country's security operations centre would need to take control of internet traffic to stop its citizens from crashing the internal infrastructure. We possibly saw this in the failed Turkish coup a few weeks ago, where YouTube and social media went completely offline inside the country.

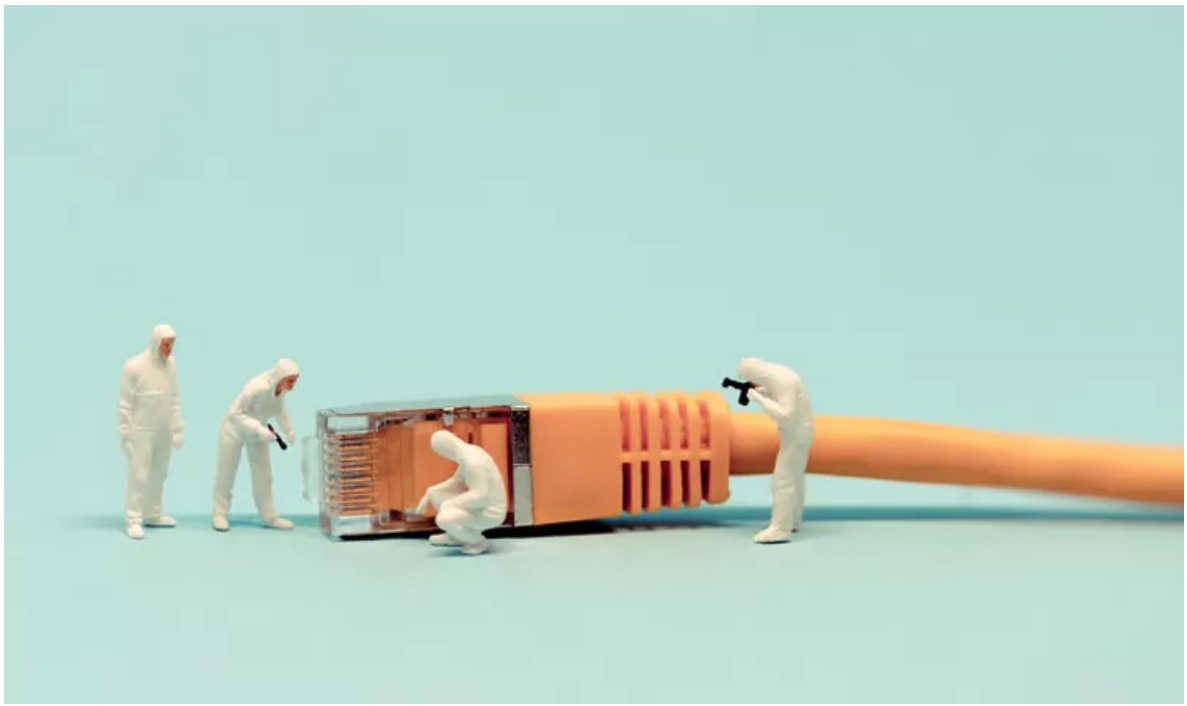
Phase two: Analysis of attack: security analysts would be trying to figure out how to cope with the attack without affecting the internal operation of the network.

Phase three: Observation and large-scale control: the authorities would be faced with countless alerts about system crashes and problems. The challenge would be to ensure only key alerts reached the analysts trying to overcome the problems before the infrastructure collapsed. A key focus would be ensuring military, transport, energy, health and law enforcement systems were given the

highest priority, along with financial systems.

Phase four: Observation and fine control: by this stage there would be some stability and the attention could turn to lesser but important alerts regarding things like financial and commercial interests.

Phase five: Coping and restoring: this would be about restoring normality and trying to recover damaged systems. The challenge would be to reach this phase as quickly as possible with the least sustained damage.



Mission: recovery. kirill_makarov

State of play

If even the security-heavy US is concerned about its grid, the same is likely to be true of most countries. I suspect many countries are not well drilled to cope with sustained DDoS, especially given the fundamental weaknesses in DNS servers. Small countries are particularly at risk because they often depend on infrastructure that reaches a central point in a larger country nearby.

The UK, it should be said, is probably better placed than some countries to survive cyber warfare. It enjoys an independent grid and GCHQ and the National Crime Agency have helped to encourage some of the best private sector security operations centres in the world. Many countries could probably learn a great deal from it. Estonia, whose infrastructure was disabled for several days in 2007 following a cyber attack, is now looking at moving copies of government data to the UK for protection.

Given the current level of international tension and the potential damage from a major cyber attack,

this is an area that all countries need to take very seriously. Better to do it now rather than waiting until one country pays the price. For better and worse, the world has never been so connected.

UK **US** **Cyber warfare** **GCHQ** **Estonia** **NCA** **Cyber-attack** **National grid** **network** **denial of service** **DDoS**