Information Security Now – 49

And Nation Shall Make War Unto Nation

John Mitchell

The original text from the Biblical book of Micha actually reads, “nation shall not lift up a sword against nation, neither shall they learn war any more". This was adopted by the BBC for their motto, “nation shall speak peace unto nation”. However, The Roman writer Publius Flavius Vegetius Renatus, wrote in the late 4th century CE, “In time of peace prepare for war”. But what kind of war should we be preparing for?

One of our national broadsheets recently reported that, “traffic lights could be hacked by Russia to potentially cause road disruption and accidents”. The newspaper had taken a selective quote made by General Sir Christopher Deverell, who also said, “a lot of our capabilities in society depend on our control systems which are accessible by cyberspace. So, you can imagine threats to power stations, threats to air traffic control, threats to transport systems. We need to be able to defend ourselves against them.” However, despite his far wider dire warnings regarding the impact of a cyberattack on our infrastructure, the headline was the threat to traffic lights. Which just about reflects the level of thought being applied to the very serious problem of the cyber threat to our national infrastructure.

When the Secretary of State for Defence says that a kinetic response may be an appropriate reply to a cyberattack, you begin to wonder if the government has any real idea of what a cyberattack can achieve. It has long been held that the next war will be won by the country with the fastest computers, but if those computers are rendered inoperative by a pre-emptive cyberattack, then the ability to initiate a kinetic response may be severely limited; especially if you do not know who was responsible for launching the attack. Tracing the launch point of an incoming missile is a trivial exercise in applied math. Tracing the source of a distributed denial of service attack is not. Combine this with our proven ability to self-deny our own services (BA, TSB and VISA spring to mind), then we may not even realise that a cyberattack is happening until it is too late to respond.

Some sixty years ago, my eldest brother served in the Royal Signals. One of his jobs was to jam enemy radio transmissions; an early form of a denial of service attack. Another role was to provide support for precision air attacks by providing radio signals from a few geographically dispersed sources which converged above the target; an early form of hitting a particular IP address. So, nothing in today’s cyber warfare is particularly new, it’s the technology which has changed: becoming more sophisticated, faster and world-wide. The playing field has also been levelled. It may cost billions to acquire a nuclear capability, or train and equip an army, but only thousands to ‘rent’ several million compromised computers to conduct a devastating attack on a nation’s infrastructure. Centralisation is the bane of modern infrastructure. During World War Two, every locomotive had its own power supply which was driven by coal and there were thousands of gas and electricity power stations which were also driven by coal. Britain had abundant coal reserves so to destroy the nations transport and power infrastructure it was necessary to destroy every node. Now, with centralisation, a dependency on external sources, GPS and the internet, we are vulnerable to denial of service attacks on our infrastructure which were unimaginable only two decades ago. Removing GPS stops driverless vehicles and the associated distribution system, but people die without heat, light, the ability to buy provisions and the facilities to cook them, even if they are available in the first place. My gas heating will not operate without electricity and neither will our infrastructure. So, my attack would be on our electricity infrastructure. No electricity, no network. No network, no ability to communicate between devices. No communication, no effective control of our power distribution. Stansted airport stopped operating because a lightning strike knocked out the electricity to its refuelling pumps. This was a localised incident but imagine this across the nation.

You will know of Denial of Service (DoS) attacks and of DDoS where the attack comes from distributed locations, but I have coined the acronym SIDoS which stands for Self Inflicted Denial of Service. Recent examples being BA, TSB and VISA and to a lesser extent the London Stock Exchange. Who needs an external attack when companies seem to have the urge to commit IT suicide on a regular basis? Which takes me back to the problem as to how could we identify the source of an attack on our infrastructure sufficiently early to react to it when it may be simply stupidity on behalf of the infrastructure supplier itself? And why should it be an external attack when it could be a “sleeper” inside the IT department. Trust, but verify, is the audit motto and based on experience I have severe doubts regarding the integrity of various IT staff that I have come across, some of whom have ended their careers in prison. However, when I raised my concerns with senior management I received the usual litany of responses ranging from outrage to questions regarding my sanity, but complacency was the more usual response, coupled with the comment that good staff are hard to find. Indeed, but our national infrastructure and I include finance as a component of this, is a strategic asset which must be protected.

The recent GDPR legislation imposes fines of up to £17 million, or 4% of global turnover for inadequate protection of personal data, but this is unlikely to deter an external attacker and the recent SIDoS debacles indicate that our tactical defences in the cyber world are woefully inadequate. If you want a government job, then you must be vetted which was fine when the government controlled our infrastructure, but today the important stuff is outside of government control and without adequate vetting processes. Pogo the possum’s cartoon promoting the first annual observance of Earth Day in 1970 – “We have seen the enemy and he is us” - is just as apt to the IT world of today as it was to the environment then. Where is the enemy when he is us? So, for our Secretary of State for Defence to imply that we could react kinetically to a cyber attack on our infrastructure indicates that he really does not understand either the nature of the threat, or how he would identify the target for his response. After all, where is the true point of origin of a DDoS attack which makes it vulnerable to a kinetic response?

John was awarded the 2017 John Ivinson medal for services to the Institute. He is a previous member of Council and the Risk, Audit and Finance Committee. He is currently Treasurer of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638