WEAPONS
An end to SP
Non lethal weapon options

FORCE PROTECTION
The fight against IEDs

SURVEILLANCE IN THE LAND DOMAIN
Wedgetail works with Army
Past, present and future programs

Authorised extract from Australian Defence Magazine
July 2012 edition
This material is copyright and may not be reproduced without the permission of the publisher.
Judy Hinz judyhinz@yaffa.com.au

ADM Exclusive FROM THE SOURCE
Dr Ben Greene Group Chief Executive
Electro Optic Systems (EOS) Holdings talks to ADM
Why are cyber warfare dogs of war so quiet?

The second annual cyber security summit covered a great deal more ground than the first. Yet it was more interesting for what it did not cover.

THE meatiest aspects this year covered managing insider threats. Dawn Cappelli from the CERT Insider Threat Center Carnegie Mellon University’s offered a well supported analysis based on some 800 case studies on what drives insider threats.

There were also the graphic surveys of the latest security nightmares by various anti-cyber crime vendors. Most Australian agencies and organisations need to let go of the quaint notion that they can still defend their perimeter from the increasingly effective intrusions, it seems.

Anne Mullins Lockheed Martin’s VP and Cyber Executive for Information Systems and Global Solutions offered a persuasive argument that organisations need to build up their security intelligence to guide their security operations.

The views of Government speakers were thoughtful but cautious, suggesting there was little change in their being behind in addressing many of the setbacks and dangers inherent in cyber intrusions this year. Australian Security and Intelligence Organisation (ASIO) and Defence Signals Directorate (DSD) speakers offered conservative and vague perspectives on the nature of the current threat.

Neither government speaker for example were willing to discuss the issue of counter-offensive cyber warfare postures, notwithstanding this was symbolically embedded in the revised ANZUS treaty. There were already several reports that confirmed that both StuxNet and the recent Flame malwares were the likely handiwork of the US. The dogs of cyberwar appear to have already been unleashed but it was not fitting forum to discuss its implications.

The solutions advanced by speakers from industry and Government centered around partnerships to improve intelligence sharing, developing “resilience” – a term that seems to be matching “agility” for the cyber security qualification we should aspire to this year. Trusted communities and even mega communities were also given considerable air time during the address and discussions.

In practice, this rang somewhat hollow when Joe Franzti of DSD indicated his organisation was yet to issue hard statistical data to quantify the extent of the threats, how they were being managed and whether Australia was winning or losing with cyber intrusions. A redacted version of Government statistics is scheduled sometime later this year, Franzti promised.

Overseas initiatives being urged by various commentators such as mandatory disclosure of data breaches are not on the agenda so we can’t be certain we are not worse off overall than we were last year.

Making sense of the Insider Threat

Dawn Cappelli, Technical Manager, Enterprise Threat & Vulnerability Management at the CERT Insider Threat Centre, Carnegie Mellon University, Pittsburgh, PA spent some 10 years dedicating her life researching malicious threats from insiders such as employees, contractors, trusted business partners.

From the Centre’s database of more than 800 case studies, Cappelli and her team identified what makes a rogue insider tick and techniques for preventing and detecting their mischief.

One third of cyber attacks are attributed to insiders and two thirds outsider. However insiders are in a superior position to invoke harm. Fortunately some patterns are emerging from her cases to indicate a cause for concern or a “red flag”, she said.

In one case, there was a large financial institution with a disgruntled systems administrator. He was furious that no bonuses were paid that year. In response he wrote malicious code that would wipe out all of the company’s files on all their servers across the US.

He then quit. A few weeks later a logic bomb went off, wiping out 10 billion files on more than 1,300 servers.

It took the company $3 million to recover. It was actually a good news story, she said. It took them only hours to recov-
er. And it did not affect their stock price.
Cappelli finds this kind of insider threat is based around revenge and tends to occur among “very technical” users. They can be upset about some matter. It may be financial. It may be a new boss, they don’t like. Technical people can be very picky about the work they do. Something makes them angry.

Unlike most other employees, these people don’t get over it. It just gets worse and worse, she said. They end up on the HR radar. They usually end up being demoted and eventually fired or they quit.

Then they decide they want revenge. They knew they were leaving or about to be fired, she said. So they set up their attack before they left. They create a way they can get back into the organisation and attack later or they set up the attack with malicious code before they leave.

Cappelli’s question for CIOs: how should they handle privileged contractors that are on the HR radar? Do you recognise they may represent an increased risk. If you do realise that risk, do you know what to do about it?

Do you have processes in place to review what those insiders were doing? Do you have the information logged so you can see what they have been doing? What accounts have they created? Backdoor accounts are very common. What code have they been writing? What have they downloaded from the Internet such as hacker tools?

She recommends organisations have in place policies, processes and the technical measures in place to enable such responses.

A second type of cyber crime by insiders concerns theft of intellectual property. A research scientist that worked at a chemical company, was disgruntled – but not as disgruntled as the system administrator discussed earlier.

This person found a new job and got his offer in August. But he did not turn in his notice until December. In those four months, he downloaded 38,000 documents containing all their proprietary information. They had a library that was a database of documents. He downloaded them one at a time.

“Think about how long that would take," Cappelli asks. “He worked up to 20 hours at a time downloading the documents. He put them on removable media and took that with him when he left in January.”

Fortunately this company looked at his computer after he left, found all those documents and became suspicious. They called the FBI who investigated and retrieved the information before he could do anything with it. That information was valued at $400 million.

Scientists, engineers, programmers or sales people typically commit these thefts, she said. They tend to steal what they work on. Usually they fall into one of two groups – “the entitled independent” – they feel a sense of ownership and when they get a new job they take it with them as “their” own.

As a mitigation strategy, she found most of these people steal the information, within 30 days of resignation. That can be 30 days before they hand in their notice or 30 days after – so there is a 60-day window of risk to focus on.

They don’t steal it and six months later leave. They steal it as they are leaving. This also suggests a mitigation strategy.

The other kind of insider theft she describes as the “ambitious leader”. They don’t just want their own stuff. They want it all. They want a whole system or a whole product line. Most of these people are steal-
“Most Australian agencies and organisations need to let go of the quaint notion that they can still defend their perimeter from the increasingly effective intrusions, it seems.”

The avenue for them to get all this information is to recruit others to help them. They end up creating a crime or espionage ring within the organisation, she said.

Some of those working with him, may not even realise what they are doing. They socially engineer them to giving them access they don’t have or don’t need.

Once again within 30 days of resignation they take it with them, she found. This means checking for stolen information when employees or contractors with critical information leave.

It’s not practical to watch everything everyone does. But when someone turns in their resignation that has access to your critical information, go back and see what they have been doing. Have they been emailing outside of the network or outside of the country or competitors with their attachments?

What have they been putting on USB drives? You can’t watch everything everybody puts on an USB drive every day. But if someone that turns in their resignation has access to your critical information, now you can go to their laptop and desktop and see what they have been doing, she said.

Use that 30-day window to devise a strategy to reduce these crimes, she counsels.

In her annual survey around 50 per cent of US organisations agree that they were the victims of at least one malicious insider attack. At least half are experiencing one per year. She also asked how many cases were handled internally and law enforcement authorities were not called in or legal action taken? Every year around three quarters of them are handled internally.

How Lockheed Martin meets Cyber threats

Anne Mullins, VP & Cyber Executive Lockheed Martin Information Systems & Global Solutions revealed that her company is not only the largest Defence Contractor in the world but also was the largest IT provider to the US Government.

In 2003 Lockheed Martin faced its first advance persistent threat in 2003 and found it was unprepared.

Since then it moved from ad hoc responses, through to being ahead of the game and producing intelligence on the nature of their attackers, their targets and tactics and protect themselves as well as protecting others.

Its key strategy was to invest in security intelligence centres to complement its security operations centres. Lockheed Martin currently has three, two in the US and one in the UK with a fourth one being considered for Australia.

These centres became the hub of Lockheed’s defence. Its breakthrough was to reframe cyber intrusions as people rather than a technology problem.
“If we understand more about what the adversaries are doing to successfully attack we can have a better posture to defend ourselves,” she told the Summit.

Each intrusion is assessed at every level on the following typologies:
- Reconnaissance
- Weaponise
- Deliver
- Export
- Install
- Command & Control
- Action on Objective

The game moves from let’s detect and stop the intrusion to detect-stop-and gather intelligence so we can be ready for it next time.

“If you detect an intrusion deep in the kill chain all the way to an objective you absolutely stop it first. Then you reconstruct the attack and you gather as much intelligence through analysis,” she said.

Her centres found many intrusions had common patterns, finger prints she could start to recognise similarities in the intrusions. They are likely to be executed by the same group of adversaries.

These were grouped together and Lockheed Martin changed its terminology from intrusions with common patterns to campaigns - a sequence of attacks that it could can develop a set of counter measures for.

“We are currently watching for 40 campaigns that we have identified over the course of 2006 through today,” she said.

Her intelligence disclosed each campaign had a distinct pattern of attack and could be tracked and checked for its relative frequency over time.

Furthermore her intelligence suggested that campaigns could be related to each other with their own set of risks and insider threats. Some campaigns merely mapped the infrastructure (reconnaissance). Adversaries behind that campaign may be content to onsell that to another campaign adversary.

“Cyber attacks contain many possibilities and its potential targets and perpetrators also cover a broad spectrum.”

In some cases, the confidence developed through Lockheed Martin’s intelligence gathering could occasionally prompt it to choose to deceive its adversaries and let them think everything is working in order to gather additional intelligence.

In summary she found commercially available products were generally inadequate not enough.

“It requires more particularly smart analysts on the front line – boots on the ground to address this problem,” she said.

What the cyber attacks really mean under ANZUS

Last year’s amended ANZUS treaty included new passages concerning cyber attacks. But these have been misunderstood according to Dr Andrew Davies, of the Australian Strategic Policy Institute.

It includes the bold declaration

“Our Governments share the view that, in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.”

At one level that is not that significant. They’ll consult and decide what to do. This picks up the language of the ANZUS treaty itself, Davies outlined.

“An attack is an attack, whether it’s in the land sea or air. Cyberspace is just another space,” Davies said.

However its practical implications are less clear.

Articles III, IV and V of the treaty are relevant:

Article III: The Parties will consult together whenever in the opinion of any of them the territorial integrity, political independence or security of any of the Parties is threatened in the Pacific.

Article IV: Each Party recognizes that an armed attack in the Pacific Area on any of the Parties would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional processes...

Article V: For the purpose of Article IV, an armed attack on any of the Parties is deemed to include an armed attack on the metropolitan territory of any of the Parties, or on the island territories under its jurisdiction in the Pacific or on its armed forces, public vessels or aircraft in the Pacific.

Davies notes that the treaty distinguishes between threats of security and threats of armed attack.

“They consult when they are threatened, but they act to meet the common danger when they are attacked,” he said.

So the joint statement on Cyber is more about Article III concerning threats to security rather than IV or V. He concludes a popular suggestion that this meant a cyber attack could trigger a military response under ANZUS was mistaken.

It requires deciding what constitutes a “cyber attack” as it’s more subtle than armed conflict.

Cyber attacks contain many possibilities and its potential targets and perpetrators also cover a broad spectrum. The targets could range from community, business, critical civilian infrastructure, whole of Government structure up to Instruments of state power (military) – the latter which comes closest to an attack on sovereignty.

Davies adds that Defence Minister Ste-
“He argues the real message of ANZUS was for China: Cyber attacks are unacceptable and it will attract a response.”

phen Smith’s gloss on the reform is revealing as well:

“We are talking here at a level that is much higher than using cyberspace to steal commercial or state secrets. We’re talking about a significant attack upon the communications fabric of a nation... In particular to thwart the communications system of the military – national security apparatus, the national security arrangements of a country.”

This sets the bar very high and still leaves open questions such as whether the attack has to come from another state or would a state sponsored attack against civilian infrastructure fall inside or outside of ANZUS.

It’s also unclear how one measures the severity of an attack, Davies said. Would a half hour outage of our air defence system caused by an external act constitute a significant attack? Or would it need to be accompanied by other hostile activity?

Even where there is an event to trigger the provisions. What is a reasonable response, he asks. Armed attacks are clear – a response in kind would be appropriate. But what if the attack comes from a non-State actor? What’s appropriate response then?

Davies counsels caution as there’s an overarching risk that we may be promoting cyber above its appropriate status.

In practice, Davies notes there are data backups and redundancies in most Western countries to mitigate the worst of these attacks. Even in 9-11 attacks, shutdown of the NY stock exchange only lasted some four trading days.

Like other Government speakers Davies concedes there was little evidence to date of such acts of cyber terrorism.

As the threshold set for the cyber attack has been set so high in ANZUS, Davies concludes it’s hard to see it ever being used to trigger the provision.

He argues the real message of ANZUS was for China: Cyber attacks are unacceptable and it will attract a response. Not necessarily a military response but it won’t go unnoticed.

Conclusions
At the end of the two days there were a key keys messages for delegates to take home from the 2nd Annual ADM Cyber Security Summit. Cooperation in terms of sharing threat data is paramount despite the closed nature of the space. The insider threat data is paramount despite the closed nature of the space. The insider threat can be much more harmful than an external one and needs a holistic approach from the entire enterprise, not just the IT department, to be successful. And no government or company is an island. The sense of community at the event was palpable, as was the feeling that it will always be the people and their motives that are the threat in this war rather than the tools.