Now Bimonthly

CBRNE Newsletter Terrorism

Volume 41, 2012

"Anonymous" hackers target US security think tank

By Cassandra Vinograd

Source: http://www.businessweek.com/ap/financialnews/D9RRNNP80.htm

Hackers with the loose-knit movement "Anonymous" claimed on Sunday to have stolen a raft of emails and credit card data from U.S.-based security think tank Stratfor, promising it was just the start of a weeklong, Christmas-inspired assault on a long list of targets.

Anonymous boasted of stealing Stratfor's confidential client list and mining it for more than 4,000 credit card numbers, passwords and addresses. The real threat appeared posed to individual employees of government agencies and private companies, and one alleged hacker said the goal was to use the credit data to pilfer a million dollars and give it away as Christmas donations.

Images posted claimed to show receipts, and victims confirmed to The Associated Press unauthorized credit card transactions linked to their accounts.

"Not as many as you expected? Worry not, fellow pirates and robin hoods. These are just the "A"s," read a message posted online that encouraged readers to download a file of the hacked information.

The flood of leaked data started when a Twitter account tied to Anonymous posted a link to what they said was Stratfor's tightly-guarded, confidential client list. Among those on the list: The U.S. Army, the U.S. Air Force and the Miami Police Department.

The rest of the list, which the hacking movement said was a small slice of its 200 gigabytes worth of plunder, included banks, law enforcement agencies, defense contractors and technology firms such as Apple and Microsoft.

"Not so private and secret anymore?" the group taunted in a message on the microblogging site, warning of more mayhem to come.

Austin, Texas-based Stratfor provides political, economic and military analysis to help clients reduce risk, according to a description on its YouTube page. It charges subscribers for its reports and analysis, delivered through the web, emails and videos.

Lt. Col. John Dorrian, public affairs officer for the Air Force, said that "for obvious reasons" the Air Force doesn't discuss specific vulnerabilities, threats or responses to them.

"The Air Force will continue to monitor the situation and, as always, take apporpriate action as necessary to protect Air Force networks and information," he said in an email.

Miami Police Department spokesman Sgt. Freddie Cruz Jr. said that he could not confirm that the agency was a client of Stratfor, and he said he had not received any information about

any security breach involving the police department.

Anonymous said it was able to get the credit details in part because Stratfor didn't bother encrypting them -- an easy-to-avoid blunder which, if true, would be a major embarrassment for any security-related company.

Hours after publishing what it claimed was Stratfor's client list, Anonymous tweeted a link to encrypted files online. It said the files contained 4,000 credit cards, passwords and home addresses belonging to individuals on the think tank's private client list.

It also linked to images online that it suggested were receipts for charitable donations made by the group manipulating the credit card data it stole.

"Thank you! Defense Intelligence Agency," read the text above one image that appeared to show a transaction summary indicating that an agency employee's information was used to donate $250 to a non-profit.

One receipt -- to the American Red Cross -- had Allen Barr's name on it.

Barr, of Austin, Texas, recently retired from the Texas Department of Banking and said he discovered last Friday that a total of $700 had been spent from his account.

Barr, who has spent more than a decade dealing with cybercrime at banks, said five transactions were made in total.
"It was all charities, the Red Cross, CARE, Save the Children. So when the credit card company called my wife she wasn't sure whether I was just donating," said Barr, who wasn't aware until a reporter with the AP called that his information had been compromised when Stratfor's computers were hacked.
"It made me feel terrible. It made my wife feel terrible. We had to close the account."
Stratfor said in an email to members that it had suspended its servers and email after learning that its website had been hacked.
"We have reason to believe that the names of our corporate subscribers have been posted on other web sites," said the email, passed on to The Associated Press by subscribers. "We are diligently investigating the extent to which subscriber information may have been obtained."
The email, signed by Stratfor Chief Executive George Friedman, said the company is "working closely with law enforcement to identify who is behind the breach."
"Stratfor's relationship with its members and, in particular, the confidentiality of their subscriber information, are very important to Stratfor and me," Friedman wrote.
Repeated calls to Stratfor went unanswered Sunday and an answering machine thanked callers for contacting the "No. 1 source for global intelligence." Stratfor's website was down, with a banner saying "site is currently undergoing maintenance."
Wishing everyone a "Merry LulzXMas" -- a nod to its spinoff hacking group Lulz Security -- Anonymous also posted a link on Twitter to a site containing the email, phone number and credit number of a U.S. Homeland Security employee.
The employee, Cody Sultenfuss, said he had no warning before his details were posted.
"They took money I did not have," he told The Associated Press in a series of emails, which did not specify the amount taken. "I think why me? I am not rich."
One member of the hacking group, who uses the handle AnonymousAbu on Twitter, claimed that more than 90,000 credit cards from law enforcement, the intelligence community and journalists -- "corporate/exec accounts of people like Fox" news -- had been hacked and used to "steal a million dollars" and make donations.
It was impossible to verify where credit card details were used. Fox News was not on the excerpted list of Stratfor members posted online, but other media organizations including MSNBC and Al Jazeera English appeared in the file.
Anonymous warned it has "enough targets lined up to extend the fun fun fun of LulzXmas through the entire next week."
The group has previously claimed responsibility for attacks on companies such as Visa, MasterCard and PayPal, as well as others in the music industry and the Church of Scientology.

Associated Press writer Jennifer Kway in Miami, Ramit Plushnick-Masti in Houston, Texas and Daniel Wagner in Washington, D.C. contributed to this report.

2012 is an Olympic year: get prepared for Olympic Cybercrime too

Source: http://www.securitypark.co.uk/security_article267083.html

With 2012 an Olympic year and athletes around the world limbering up to compete, cyber criminals too are preparing for the next twelve months warns Trusteer. Using the intelligence Trusteer's gathered of the criminals mind, and the weapons at their disposal, this leading provider of cybercrime prevention solutions today gave its guidance of how it expects threats will morph during 2012.

Amit Klein, CTO for Trusteer explains, "Cybercriminals are successfully defeating security controls across the globe and in all industries. They have moved from the shotgun approach to a marksman's methodology, becoming focused on the institutions they target. More organised then ever before, tomorrow's cybercriminal studies their prey and learns their security controls so then can bypass them and commit fraud.

While the Olympic's may be a distraction, it's vitally important that security professionals don't take their eye of the prize – to play these fraudsters at their own game, and win gold."

Trusteer has made five leading predictions for 2012:

- Prediction 1 – 2012 will see new multipurpose multi functional malware:
  Trusteer predicts malware, originally designed for one purpose, will evolve to pose a new threat with a malicious undertone. Non-financial viruses will morph to become financial malware and be used to commit online banking fraud. Conversely, existing financial malware, will adopt features introduced in non-financial APT attacks. Over the next twelve months perimeters will face an onslaught from various sources, viruses going financial, APT style technologies in ZeuS code derivatives manipulated by new coders and in other commercially available malware kits (e.g. Spyeye).
- Prediction 2 – We're on the verge of malware globalisation
  Next year cybercriminals will realise their dreams of global domination as Trusteer expects to see widespread resale and repackaging of malware. This means code, originally designed specifically to target one geographical location, will be adopted and translated to target other regions or even countries. The end result will see terms such as 'regional malware' and even 'malware free countries' cease to exist as everyone, regardless of where they are, comes into the sights of the criminal fraternity.
- Prediction 3 – Cyber criminals will up their game and improve evasion techniques
  Ultimately a cyber criminal's focus is on infecting the user's PC and to remain undetected for as long as possible. It makes sense, therefore, that they will continue to improve their evasion techniques to 'hide' the rogue program or mimic that of another program. But be warned, where evasion techniques are unsuccessful, fraudsters will resort to developing malware designed to attack and destroy existing protection, with the premise that the organization, and its users, may not notice they're vulnerable to attack.
- Prediction 4 - Personal information, disclosed on social networks, will be used in social engineering attacks against the enterprise
  Fraudsters, all too aware of the valuable intelligence freely available social networks, are starting to mine these data sources capturing the personal details needed to successfully complete social engineering attacks. Trusteer predicts this will manifest itself over the coming year as an enterprise issue. As a crude example, if an enterprise uses a 'secret question' for password retrieval, it's feasible that an individual's answers could be researched via the net, the password reset and the legitimate account used to compromise the organisation.
- Prediction 5 – the move to SaaS allowing malware attacks on enterprise applications
  Many organisations, in an effort to reduce cost of enterprise application have moved to SaaS. However, as part of this process, many have outsourced services to external websites without first carefully considering the security risks it presents. While the damage that can be done has not yet been evident, Trusteer's prediction is that it will become apparent over the next 12 months. Its belief is that many organisations will spend 2012 fighting flames, backtracking and perhaps having to withdraw these services.

Key principles in fighting 2012 cyber crime

Searching for security solutions that can turn the table on cyber criminals and maintain the upper hand requires a closer look at the shared attack vectors of successful cyber crime schemes.

- First, malware residing on the machine abuses the trust a user places in the browser and the rendered site, through which

fraudsters can initiate an endless number of social engineering attack variations.
- Second, malware that has free access to application and system resources will eventually leverage technology and social engineering to penetrate any security control.

Amit concludes, "Cybercrime will eventually prevail if malware is allowed to infect machines and remain undetected and uninterrupted. Over time cybercrime prevention can simply not coexist with malware infected machines. Consequently, effective sustainable security requires cyber crime intelligence that identifies new malware attack and infection behaviours, complemented by the ability of the security control (technology and process) to quickly adapt to and defeat new threats. Forewarned is forearmed, and you've been warned."

First EU-Report on Maritime Cyber Security

Analysis highlights essential key insights, as well as existing initiatives

Source:http://www.darkreading.com/security/news/232300837/first-eu-report-on-maritime-cyber-security.html

BRUSSELS and HERAKLION, Greece, December 20, 2011 /PRNewswire/ --

ENISA has published the first EU report [http://www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector] ever on cyber security challenges in the Maritime Sector. This principal analysis highlights essential key insights, as well as existing initiatives, as a baseline for cyber security. Finally, high-level recommendations are given for addressing these risks.

Cyber threats are a growing menace, spreading to all industry sectors that rely on ICT systems. Recent deliberate disruptions of critical automation systems, such as Stuxnet [http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis], prove that cyber-attacks have a significant impact on critical infrastructures. Disruption of these ICT capabilities may have disastrous consequences for EU Member States' governments and social well-being. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level.

Some key findings of the report [http://www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector] ;

- Maritime cyber security awareness is currently low, to non-existent. Member States are thus highly recommended to undertake targeted maritime sector awareness raising campaigns and cyber security training of shipping companies, port authorities, national cyber security offices, etc. - Due to the high ICT complexity, it is a major challenge to ensure adequate maritime cyber security. A common strategy, and the establishing of good practices for technology development and implementation of ICT systems would therefore ensure "security by design" for all critical maritime ICT components. - As current maritime regulations and policies consider only physical aspects of security and safety, policy makers should add cyber security aspects to them. - ENISA strongly recommends a holistic, risk-based approach; assessment of maritime-specific cyber risks, as well as identification of all critical assets within this sector. - As maritime governance is fragmented between different levels (i.e. international, European, national), the International Maritime Organisation together with the EU Commission and the Member States should align international and EU policies in this sector. - Better information exchange and statistics on cyber security can help insurers to improve their actuarial models, reduce own risks, and thus offer better contractual insurance conditions for the maritime sector. Information exchange platforms, such as CPNI.NL, should be also considered and by Member States to better communications.

The Executive Director of ENISA, Professor Udo Helmbrecht comments;

"This report positions maritime cyber security as a logical and crucial next step in the global protection efforts of ICT infrastructure."

Maritime figures

- 90% of the EU's external trade and more than 40% of the internal trade take place via maritime routes.

Consequently, securing the maritime sector's critical infrastructure and the movement of vital goods, e.g. food and health supplies is a priority area for Europe.

NOTE: Read/download the full report at the Newsletter's website – "CBRNE-CT Papers" section

Will Kim Jong Un be for cyberwarfare what his dad was for nukes?

Source: http://www.csoonline.com/article/696930/will-kim-jong-un-be-for-cyberwarfare-what-his-dad-was-for-nukes-

The death of North Korean dictator Kim Jong Il has understandably set neighboring South Korea and other countries in the region on edge. But should it put the western world on high alert as well, for possible cyberattacks?

Two cyber security experts have different views on the matter.

There is general agreement that the transition of power could bring significant instability to the region. While the dictator's son, Kim Jong Un, was named by his father to succeed him, the twenty-something Kim has had only two years to be groomed for the position, while his father had 14. He was made a four-star general by his father, but has never served in the military.

And even if the younger Kim does take power seamlessly, there is speculation that he may deliberately act aggressively to quash even the thought of an "Arab Spring" type of rebellion, to consolidate his power and establish a reputation throughout the world that he will be just as unpredictable and threatening as his father.

South Korea's largest news agency, Yonhap, reported that the country had put its military on high alert.

Korea Communications Commission (KCC) raised the cyber alert to the third-highest level over the weekend and stepped up monitoring on distributed denial-of-service attacks, hacking incidents and other assaults via the Internet.

John Linkous, vice-president and chief security and compliance officer of eIQnetworks, says this amount to "a strong possibility" that North Korea could launch cyberattacks against the U.S.

And he says neither private industry nor government may be adequately prepared.

"On the commercial side, if you look at all the successful cyberattacks over the past year, businesses are not prepared," he says, noting that most of those attacks are from smaller organizations, not nation states.

"On the federal side, I would like to think we are prepared, but we probably are not," Linkous says. "We have so many infrastructures spread out over the world that economically and mathematically it's almost not feasible."

He notes that Vivek Kundra, former U.S. chief information officer, gave government cybersecurity a "B" grade before he left office in August.

"The (attack) vectors themselves are not that sophisticated, but they don't need to be," he says. "The reality is that this is a nation that clearly views itself as world leader and wants to assert itself in every way. Cybersecurity is a big part of that.

But Gary McGraw, chief technology officer for Cigital, doesn't see the political instability in the country as a direct threat, and says he doesn't think North Korea has the ability to launch a disabling cyberattack.

"A few times in the past North Korea has been blamed for stuff without much evidence, and it wasn't much beyond denial of service anyway," he says.

McGraw says the kind of attacks that might come from North Korea, are the kinds of things that Google and Amazon probably wouldn't even notice, and if they did, they would have no trouble shutting them down."

He says while cyberwar should be taken seriously, some of the fears about it are the result of hype.

North Korea, he says, has much more serious internal problems to confront.

"Why are we wringing our hands over cyberwar?" he asks. "We ought to be wringing our hands over the fact that

they can't even feed their own people."

McAfee releases 2012 cyber threat predictions

Source: http://blogs.mcafee.com/consumer/2012-mcafee-threat-predictions-consumers

The cyberthreats organizations and individuals are likely to face in 2012 will resemble those they faces in 2011, only more so; among the increased threats: attacks on critical infrastructure, mobile devices and consumer electronics, and politically motivated attacks

McAfee has released its list of the major cybersecurity threats organizations and individuals are likely to face in 2012. The company says that for the most part, 2012 looks like it will contain an elevation of many of the threats recently seen to be gaining momentum. Here are the predictions:

1. Disrupted utilities like water and power: earlier in the year a Southern California water systems hired a hacker to find vulnerabilities in its computer networks. The hacker had no trouble seizing control of their equipment and adding chemicals to the drinking water, and do all this in day.

McAfee says that many industrial and national infrastructure networks were not designed for modern connectivity, making them vulnerable. "We expect attackers to take advantage of the situation in 2012, if only for blackmail or extortion, but in a worst-case scenario public utilities such as water and electrical services could be disrupted."

2. Affecting political change through hacktivism: hactivism is the use of computers or computer networks to protest or promote political change. A great example of this is the "Anonymous" group which was active last year doing high profile activities such as briefly taking down New York Stock Exchange's Web site in support of the Occupy Wall Street protests.

McAfee says it expects more organized digital disruptions to come in 2012.

3. More spam in consumers' inboxes: the new trend in spamming is sending e-mails from advertising companies that obtain their e-mail lists through shady but legal means. They may buy the lists from companies that are going out of business or partner with other advertising entities or mail-list providers without taking into account privacy policies.

McAfee notes that spammers can do this because under the U.S. CAN-SPAM Act advertisers are not required to receive consent before sending advertising. Since this method is cheaper and less risky than bombarding consumers with spam from networks of compromised computers, this activity is likely to continue to grow through 2012, possibly resulting in more spam in inboxes.

4. Malware aimed at mobile phones: Cybercriminals are now testing their creativity with mobile malware in the form of malicious applications. Once downloaded, they can deliver a variety of ads or even send expensive text messages from your phone. They are using botnets — a collection of compromised computers that have traditionally been used to do things like send spam — to target mobile platforms.

McAfee says that mobile malware is not common now, but that it expects

these attacks to increase through next year.

5. Compromised cars, GPS trackers, and other devices: cybercriminals are now targeting embedded operating systems or even hardware to gain control of everything from cars to GPS trackers and medical equipment. They can do this two ways — either through infiltrating the device when it is being manufactured or through the easier route of tricking users into downloading malware that can penetrate the "root" of the system.

McAffee expects hackers to become more effective in 2012 and beyond, potentially affecting systems such as consumer electronics.

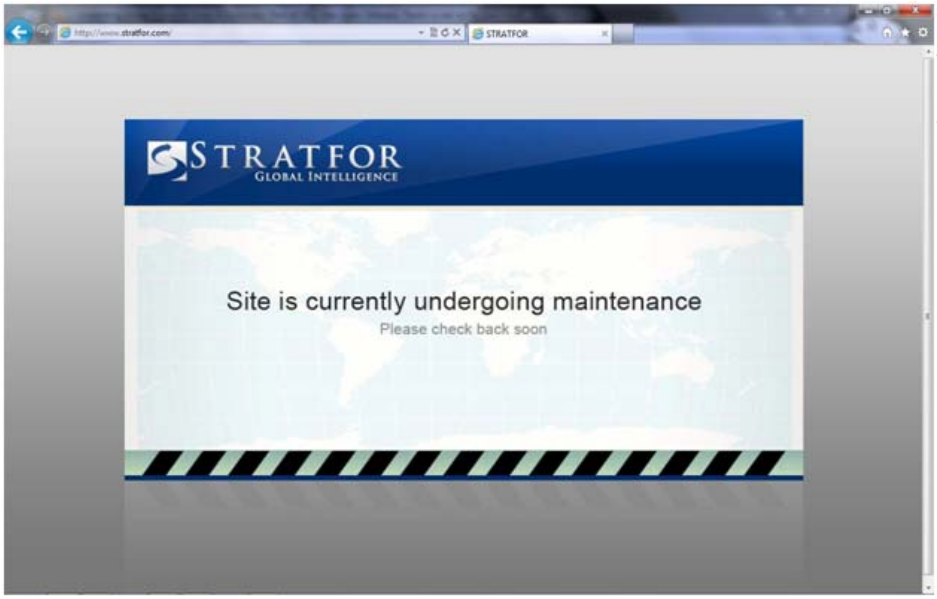
6. Cyberwar: there has recently been an increase in high-tech spying and other cyber techniques to gain intelligence, even if on a small scale. Many countries are now realizing the crippling potential of cyberattacks against critical infrastructure, and realize how hard they are to defend. This dangerous possibility is out there.

Stratfor - Lessons Learned

By Gregory W. MacPherson, Computer Security Expert, CISSP, etc.
Source: http://seclists.org/isn/2012/Jan/6

The stratfor.com hack is old news by now, so what lessons, if any, are there to be learned from this high profile data spill?

To review, stratfor.com private data including credit cards, user accounts, and passwords was dumped on pastebin.com on Christmas Day, 2011. The data spill exposed not only tens of thousands of users to potential identity theft but more importantly exposed the security practices of those users, as well as the security practices of stratfor.com.



A review of the data and of the incident suggests several points worthy of consideration. The data was compromised using either a cross site scripting or SQL injection attack. From this fact one might conclude that application security trumps data security, and in this case one would be correct. Of course if the administrators of stratfor had practiced basic data security techniques such as encrypting data at rest, then the sensitive PII of tens of thousands of users might not be on display for the world today. While the Web site did incorporate SSL for user transactions, the account and credit card information existed in a data store in clear text rather than as encrypted hash values. Once the exterior security of the site was breached, regardless of the method, the entire site was compromised. This is referred to in the vernacular as "hard exterior, soft chewy inside" and is an unfortunate and prevalant security strategy. Numerous discussions of layered security have addressed the point, therefore I will not belabor it here. Suffice to say that the administrators of stratfor.com now may be viewed as idiots for not following well documented and oft published best practices for computer security.

A heuristic study of the user account credentials reveals another salient fact: stratfor users are idiots as well when it comes to security. The password distribution curve for stratfor includes multiple uses of passwords of one character, two characters, three characters, ad nauseum. Additionally dozens of "joe" accounts - accounts where the password echoed the username - are in evidence. Stratfor.com made no effort to

enforce a strong password policy - a few lines of JavaScript would have sufficed - and as a consequence we find embarrassing examples such as username stratfor, password stratfor. One real benefit of this data breach is that it illustrates a real world example of the poor choices that users make when it comes to computer security. Strong security must be enforced, not optional, and allowing users to decide whether the security measures inconvenience them leads to situations such as the current topic of discussion.

A third point for consideration is the situation where multiple users with credentials ending in TLDs such as dot-edu, dot-gov, and dot-mil utilized passwords on stratfor.com that echo their credentials on their more sensitive home sites. One would like to think that people who boast of academic, government, or military credentials would be more cognizant of their responsibility to protect the privileged information entrusted to them, but apparently they too, despite their august credentials, are idiots when it comes to authentication credentials and the management thereof. Suffice to say that dot-mil sites routinely employ two-factor authentication to prevent compromises of this exact sort. Some government sites also employ two-factor authentication methods, and possibly a few academic sites do as well. For those sites which rely solely on the arcane userid and password combination, I suspect that this holiday season was less than merry as their security staff worked late to try and head off the inevitable compromises that would result after dozens of credentials were published.

Finally, not to put too fine a point on it, but the strategy employed by the villains in this scenario - security by embarrassment - remains the sole successful motivational strategy when it comes to computer security. Businesses, academic institutions, government and military all continue to denigrate the role for security in the infrastructure, allocating it the moniker of a "cost of doing business" and placing it strategically somewhere near the bottom of the priority list above performance tuning and documentation. Unfortunately incidents such as the most recent compromise continue to illustrate that business people are idiots when it comes to technology. Decision makers refuse to accept that competent adversaries exist and that those adversaries are both capable and willing to exact this sort of toll on their ability to do business.

Stratfor.com will recover from the recent compromises, and will have a stronger and more robust security posture - for a while. Then business decision makers will become complacent and will look for areas to "cut costs" - and security once again will be relegated to the position of the "kid who gets picked last for the team sport".

If any lesson is to be learned, business people should look at this incident as an example of "the emperor has no clothes" and be more amenable to the entreaties of their technologists and security architects who berate the CFOs and CEOs for funds to allow them to protect the enterprise. While the primary goal of any enterprise - whether private or public - is to "sell widgets". However no store owner of any repute would leave his shop unlocked, unguarded, and unprotected in a "bad neighborhood" - and the Internet is the worst neighborhood possible. At the same time, store owners must be wary of charlatans and snake oil sales people, so choose your computer security expert wisely.

Security best practices have been well documented. It's time for a course in computer security to be added to the lexicon of the business graduate. To neglect the necessity of securing the enterprise properly is for a store owner to leave their cash register unguarded during a riot - idiocy.

Japan develops virus to counter cyber-attacks: But can it be used?

Source:http://www.zdnet.com/blog/asia/japan-develops-virus-to-counter-cyber-attacks-but-can-it-be-used/635

Japan's Ministry of Defense has commissioned Fujitsu to create a 'search and destroy' virus to counter cyber-attacks, but current legislation prevents its use.

The Japanese Ministry of Defense has revealed its latest project to tackle

hacking: a 'seek and destroy' virus designed to track and disable the source of cyber-attacks.
The project, launched in 2008, cost $2.3 million over three years. Several companies competed for the contract, but Fujitsu was eventually commissioned to develop the new 'cyberweapon'.
The virus has already undergone testing in a closed network environment.
The major feature of the virus is the ability to trace down the source of cyber attacks, including 'spring board' computers used in the attack. The idea is that the 'cyberweapon' will also be able to disable the attacking program and collect information.
According to *The Daily Youmuri*, the virus is particularly effective against distributed denial-of-service attacks, a common form of cyber attack where hackers bombard websites with enormous volumes of data, forcing sites to shut down.
Unfortunately, Japan's Ministry of Defense still has several hurdles to jump before this project can be utilised.
Current Japanese legislation prohibits an 'offensive' retaliation to cyber-attacks, meaning that the current laws will need to be updated before the cyberweapon could be used.
Equally, creating a virus of this sort would violate a clause banning virus production in the Criminal Code.
Ministry officials said that they presently have no authorisation to use cyberweapons to counter cyber-attacks from abroad, unless they are properly defined in defence laws.
Japan's lack of defence when it comes to cyberattacks has drawn criticism recently. A senior ministry official stated that: "Japan will be the only nation with no effective cyber-attack countermeasures unless the legal issue is settled as soon as possible".
Minoru Tereda, a former parliamentary defense secretary, said it is, "regrettable", adding: "Even if cyberweapon development continues, there will be no way to fully take advantage of it".
Fujitsu has declined to comment on the project, but Ministry has said so far that it is not considering outside applications for the program at this point.

Kaspersky Lab Cyberthreat 2012 forecast

Source: http://mybroadband.co.za/news/security/40779-kaspersky-lab-cyberthreat-2012-forecast.html

Kaspersky Lab have picked out the key trends of the past 12 months and compiled a report that highlights the major new features on the security landscape for 2012.
The most significant stories of 2011 according to Costin Raiu, Director of Kaspersky Lab's Global Research & Analysis Team, were:

1. The Rise of 'Hacktivism' – one of the major trends of 2011, and no doubt it will continue into 2012.
2. The HBGary Federal Hack – how weak passwords, old software systems, and use of the cloud created a security nightmare.
3. The Advanced Persistent Threat – these attacks confirm the emergence of cyber-espionage as common practice among powerful state actors.
4. The attacks against Comodo and DigiNotar – trust in certificate authorities (CA) is under threat. In the future, CA compromises may become more widespread. Besides, it is likely that more digitally-signed malware will appear.
5. Duqu and Stuxnet – state-of-the-art cyber warfare.
6. The Sony PlayStation Network Hack – the new perils hidden in the cloud. Personally Identifiable Information (PII) is conveniently available in one place, accessed over fast Internet links; ready to be stolen in case of any misconfigurations or security issues.
7. Botnet Takedowns and the battle against Cybercrime – serving notice to the cyber gangs that their scams are no longer risk-free. But every battle shows up the vast limitations of today's legal systems when it comes to a coordinated and effective approach to cybercrime.
8. The Rise of Android Malware – several factors make Android vulnerable to cybercrime: rapid growth; freely available documentation about the platform; and weak screening at Google Market, making it easy to upload malicious programs.
9. The CarrierIQ Incident – do you know exactly what is running on your mobile device? A single incident highlighted how little we know about who is in control of our hardware.

10. Mac OS Malware – the crossover of PC threats (rogue AV programs are one of the most popular malware categories for PCs) to Macs was another important trend of 2011.

"We selected these stories because they point to the major actors of 2011 who will no doubt continue to play a major role in the cyber-security blockbuster which is just around the corner," according to Raiu.

"At the moment, the majority of incidents affect companies and state organisations involved in arms manufacturing, financial operations, or hi-tech and scientific research activities. In 2012 companies in the natural resource extraction, energy, transport, food and pharmaceutical industries will be affected, as well as Internet services and information security companies," warns Alexander Gostev, author of the 2012 Cyberthreat Forecast for 2012.

Kaspersky Lab experts predict that attackers will have to change their methods in response to the growing competition among the IT security companies that investigate and protect against targeted attacks. Increased public attention to security lapses will also force the attackers to search for new instruments.

The conventional method of attacks that involve email attachments with vulnerability exploits will gradually become less effective, while browser attacks will gain in popularity.

The Kaspersky Lab forecast goes on state that hacktivist attacks on state organisations and businesses will continue in 2012 and will have a predominantly political agenda. Gostev believes this will be an important trend when compared to similar attacks in 2011. However, hacktivism could well be used as a diversionary tactic to conceal other types of attacks.

Hi-tech malicious programs such as Stuxnet and Duqu created with state support will remain unique phenomena. Their emergence will be dictated by international tensions between specific countries. In Gostev's view, the cyber conflicts in 2012 will revolve around traditional confrontations – the US and Israel versus Iran, and the US and Western Europe versus China.

More basic weapons designed to destroy data at a given time, such as kill switches, logic bombs etc. will become more popular as they are easier to manufacture. The creation of these programs can be outsourced to private contractors used by the military or other government agencies. In many cases the contractor may not be aware of the customer's aims.

In terms of mobile threats in 2012, Kaspersky Lab expects to see Google Android continue to be the target of choice for the mobile malware market as well as an increase in the numbers of attacks that exploit vulnerabilities. The emergence of the first mobile drive-by attacks and mobile botnets are also forecast.

Mobile espionage will become widespread and will most probably include data theft from mobile phones and the tracking of people using their telephones and geolocation services.

Stuxnet and Duqu part of assembly line

Source: http://www.homelandsecuritynewswire.com/dr20120118-stuxnet-and-duqu-part-of-assembly-line-researchers

Stuxnet, the highly sophisticated piece of malicious code that was the first to cause physical damage, could just be the tip of the iceberg in a massive cyberweapon manufacturing operation. According to cybersecurity researchers at Kaspersky Labs and Symantec, Stuxnet appears to be part of a larger cybersecurity weapons program with fully operational and easily modified malicious code that can be aimed at different targets with minimal costs or effort.

Since Stuxnet's discovery, the two companies have been hard at work deciphering the code and both found common digital traces for at least seven "launcher" files made from the same software platform. A launcher file is used to secretly insert malicious code onto a computer along with any additional code needed to make the payload function.

So far the seven discovered launcher files contain portions of identical source code, with minor, but critical, differences. Two of the files are known to be used by Stuxnet and two others are used by Duqu, a recently discovered intelligence gathering program thought to be a precursor to Stuxnet.

The remaining three launchers could be associated with unknown versions of Stuxnet and Duqu, or undiscovered cyberweapons currently in operation.

Costin Raiu, the director of the global research and analysis team at Kaspersky Labs, explained, "Stuxnet's creators used a [software] platform to package and deliver it, because they wanted to be able to make many cyberweapons easily and be able to change them rapidly for targeting and attack."

Raiu added, "Let's imagine you want to steal documents. You don't need the sort of sabotage capability built into Stuxnet, so you take that off. Instead, you use the same platform to create targeted malware, but perhaps focusing on espionage instead. That's Duqu."

Liam O Murchu, Symantec Security Response's manager of operations, said Symantec's research corroborates Kaspersky's findings.

"We've done the same analysis Kaspersky has, and seen the same timelines, dates, encryption keys," O Murchu said. "We think Stuxnet and Duqu are made by the same team, with the same goal…. They can change [the software weapon produced on the common platform], manipulate it, have different payloads."

Using a common platform, the code's creators can quickly and conveniently reuse software that was expensive to develop. The common platform is similar to a factory production process for building exotic cars where there are many common parts like a frame or an engine, but certain portions must be custom built. This system allows for the quick assembly of existing code to create fully-developed cyberweapons that can be modified to target new industrial control systems or evade detection.

The latest discovery of a common platform, has divided the cybersecurity community with experts disagreeing on the implications.

Don Jackson, a senior security researcher with the Dell SecureWorks Counter Threat Unit, argued that it is unlikely that the platform suggests one lab or set of researchers created all of the malicious software, instead it is more likely that different groups used the same "kit."

"Many other dimensions of the separate attacks indicate no common authorship or attribution," Jackson said.

In contrast, Ed Skoudis, the cofounder of Inguardians, a cybersecurity firm, agreed with Kaspersky and Symantec.

"It makes tremendous sense," Skoudis said. "Look at the effort needed to produce Stuxnet. You wouldn't want to do it in a way that was one-off. You would want to produce a process that could reuse the parts, not shoot your entire cache of weapons in one attack."

As an example, Skoudis pointed to the United States and its efforts to build the first atomic bomb.

"When the U.S. built the atom bomb, it wasn't just the one. We had an infrastructure and platform for building additional weapons," Skoudis said. "Whoever built Stuxnet got a lot of money and a lot of smart people working on it. It just makes sense that creating these kinds of weapons be repeatable –and that some set of fingerprints are left behind that shows that."

Adding to the analogy, Raiu likened the Stuxnet manufacturers to a high-tech laboratory developing futuristic weapons.

"What's going on seems not so much like a weapons factory as much as a super-secret lab that creates experimental cyberweapons," he said. "It's more like they're making ion cannons or something – but for cyberwar. These are not normal line weapons, but the highest tech possible to wage cyberwar and cybersabotage."

Hackers manipulated railway computers, TSA memo says

Source: http://www.nextgov.com/nextgov/ng_20120123_3491.php?oref=topstory

Hackers, possibly from abroad, executed an attack on a Northwest rail company's computers that disrupted railway signals for two days in December, according to a government memo recapping outreach with the transportation sector during the emergency.

On Dec. 1, train service on the unnamed railroad "was slowed for a short while" and rail schedules were delayed about 15 minutes after the interference, stated a Transportation Security Administration summary of a Dec. 20 meeting about the episode obtained by *Nextgov*. The following day, shortly before rush hour, a "second event occurred" that did not affect schedules, TSA officials added. The agency is responsible for protecting all U.S. transportation systems, not just airports.

"Amtrak and the freight rails needed to have context regarding their information technical centers," the memo stated. "Cyberattacks were not a major concern to most rail operators" at the time, adding, "the conclusion that rail was affect [sic] by a cyberattack is very serious."

While government and critical industry sectors have made strides in sharing threat intelligence, less attention has been paid to translating those analyses into usable information for the people in the trenches, who are running the subways, highways and other transit systems, some former federal officials say. The recent TSA outreach was unique in that officials told operators how the breach interrupted the railway's normal activities, said Steve Carver, a retired Federal Aviation Administration information security manager, now an aviation industry consultant, who reviewed the memo.

"This TSA program is a start to bring, at a higher level, an understanding of the national impact to cyberattacks," Carver said. The U.S. Computer Emergency Readiness Team and the Pentagon's National Security Agency "have provided great information on the particular threat. They don't say how it has affected others. TSA tells you how it affected others."

The incident summary praised several TSA personnel for explaining the unfolding situation in context. When TSA investigators began to suspect the exploit was an intentional act rather than a glitch, they acted under the assumption it could present a broader danger to the U.S. transportation system, according to the memo.

"Some of the possible causes lead to consideration of an overseas cyberattack," the write-up stated. Investigators discovered two Internet access locations, or IP addresses, for the intruders on Dec. 1 and a third on Dec. 2, the document noted, but it does not say in which country they were located.

"Information stating the incidents were a targeted attack was not sent out" until midday on Monday, Dec. 5, according to the memo. The data that train operators needed to diffuse the situation was made available to them, officials wrote. Alerts listing the three IP addresses went out to several hundred railroad firms and public transportation agencies, as well as to partners in Canada.

"The processes set in place for government to work with the industry in real-time communications regarding a cyber event aligned superbly," the recap stated.

Participants in the Dec. 20 meeting included representatives from information technology firm Indus Corp., the Association of American Railroads, and Boeing Co., as well as government officials from TSA, the Homeland Security Department's cybersecurity divisions, the Transportation Department, and the U.S. Coast Guard.

But, on Monday, officials at the Homeland Security Department, which oversees TSA, said following additional in-depth

analysis, it appears that the rail infiltration may not have been a targeted attack.

"On December 1, a Pacific Northwest transportation entity reported that a potential cyber incident could affect train service," DHS spokesman Peter Boogaard said. "The Department of Homeland Security, the FBI and our federal partners remained in communication with representatives from the transportation entity in support of their mitigation activities and with state and local government officials to send alerts to notify the transportation community of the anomalous activity as it was occurring."

Based on the memo, it is unclear if other railway companies have experienced similar network incidents. Companies often are reluctant to discuss computer breaches openly for fear of scaring off customers. And, sometimes, businesses never detect the intrusions, they add.

For government to improve cyber emergency response, "the biggest thing is to start with the communications staff," Carver recommends. "There needs to be an interpreter who can take the information coming out of the U.S. CERT, take that, extract that out, and determine what it means for operations."

Rail industry representatives said they were not at liberty to discuss the contents of the government memo but said the memo was inaccurate. "There was no targeted computer-based attack on a railroad," said Holly Arthur, a spokeswoman for the Association of American Railroads. "Railroads closely monitor cyber security as a fully integrated part of both the industry's overall security plan, as well as individual company plans. Continuous coordination on cyber security occurs across the industry and with the federal government," she said.

"In addition to security measures, railroads like other high tech industries have multiple backup capabilities and ultimately manual operation procedures to address virtually any type of disruption," Arthur said.

Cyber crime 'to overtake terrorism' as top threat facing the US

Source:http://www.scmagazineuk.com/cyber-crime-to-overtake-terrorism-as-top-threat-facing-the-us/article/225613/

Iran has been identified as the main cyber threat to the United States as the office of the Director of National Intelligence (DNI) claims that intrusions are not being detected.

The report by DNI James R. Clapper identified Iran as the main danger to America's information security.

It said: “Russia and China are aggressive and successful purveyors of economic espionage against the United States. Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity. We assess that FIS (foreign intelligence services) from these three countries will remain the top threats to the United States in the coming years.”

He also claimed that FIS have launched numerous computer network operations that target US government agencies, businesses and universities, and believed that "many intrusions into US networks are not being detected".

“Although most activity detected to date has been targeted against unclassified networks connected to the internet, foreign cyber actors have also begun targeting classified networks,” he said.

On insider threats, Clapper said insiders have caused significant damage to US interests through the theft and unauthorised disclosure of classified, economic and proprietary information and other acts of espionage.

Observing the sophistication of computer network operations (CNO), Clapper said these are likely to increase in coming years. He acknowledged the two strategic challenges regarding cyber threats as: the difficulty of providing timely actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively

attributing them and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and the highly complex vulnerabilities associated with the IT supply chain for US networks.

"In both cases, US government engagement with private sector owners and operators of critical infrastructures is essential for mitigating these threats," he said.

According to ABC News, FBI director Robert Mueller said cyber espionage, computer crime and attacks on critical infrastructure will surpass terrorism as the number one threat facing the US.

He said: "I do not think today it is necessarily [the] number one threat, but it will be tomorrow. Counterterrorism – stopping terrorist attacks – with the FBI is the present priority. But down the road, the cyber threat, which cuts across all [FBI] programs, will be the number one threat to the country."

Research by NCC Group found that cyber crime originating from the UK cost the global economy more than £1.3bn in 2011, with more than 23 million hacks attempted. This placed the UK at 15th in its global hacking league table, with the US and China positioned first and second respectively.

Together those two countries are responsible for nearly 40 per cent of the world's hack attempts, costing the global economy more than $44bn each year.

Rob Cotton, NCC Group's chief executive, said: "Reading the papers each day, it's easy to think of hacking as something that happens to us from afar; that we're victims of foreign criminal gangs in developing countries. Yet hackers can be anywhere in the world, as our research illustrates, including on our own doorstep.

"Fighting this global threat will only work with global collaboration. We hear lots about governments wanting to work together and there's a strong financial motivation to find this long-suggested global solution, but progress is painfully slow."

Akamai said half of the attack traffic against its platform came from Asia, largely from Indonesia, while Taiwan and China accounted for just under 20 per cent of observed attack traffic.

Attacks from South Korea tripled, while attack traffic originating in Europe was down slightly to 28 per cent, and North and South America accounted for nearly 19 per cent. The remaining four per cent came from Africa.

Ranking countries' cyberattack preparedness

Source:http://www.homelandsecuritynewswire.com/srinfrastructure20120206-ranking-countries-cyberattack-preparedness

A new McAfee cybersecurity survey concluded

that Israel, Finland, and Sweden are leading other countries in "cyber-readiness." The report says that China, Brazil, and Mexico are among the leased cyber-prepared to defend these countries' networks against cyber attacks.

The ranking was on a continuum from one star (unprepared for cyberattacks) to five stars. No county received either five stars or one star. Israel, Finland, and Sweden received four-and-a-half stars each.

The BBC reports that the United Kingdom, with a grading of four out of five stars, ranks favorably in the survey, along with the United States, Germany, Spain, and France.

The survey was conducted by the Security and Defense Agenda (SDA) organization.

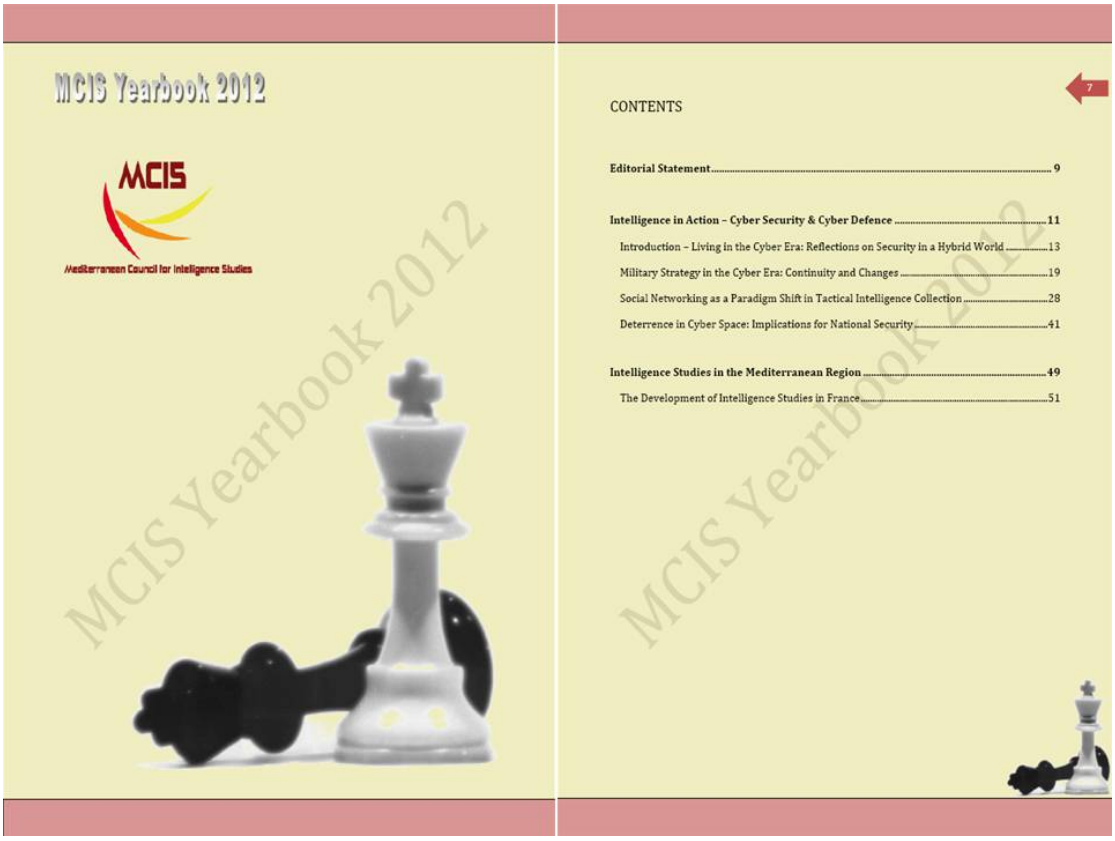
The report recommends that countries engage in more information sharing on national security issues, but experts in the field doubt this particular recommendation will be adopted. Dr. Joss Wright from the Oxford Internet Institute, while welcoming the report's findings, told the BBC he had serious doubts over the feasibility of its suggestions. "They're recommendations that people have been saying for maybe 10 years," he told the BBC. I would love to see good information sharing - but when you're talking about national security, there's a culture of not sharing. They're

not suddenly going to change 70, 100, 1000 years of military thinking."

NOTE: You can download full report from Newsletter's website – "CBRNE/CT Papers" link.

Mediterranean Council for Intelligence Studies (MCIS) – 2012 Yearbook

► Special focus in cyber-defence.



NOTE: You can download full report from Newsletter's website – "CBRNE/CT Papers" link.

Lockheed Martin's NextGen cyber lab

Contributor: Andrew Elwell

Source:http://www.defenceiq.com/defence-technology/articles/a-tour-around-lockheed-martin-s-nextgen-cyber-lab/&mac=DFIQ_OI_Featured_2011&utm_source=defenceiq.com&utm_medium=email&utm_campaign=DefOptIn&utm_content=2/14/12

Defence IQ was recently given exclusive access to Lockheed Martin UK's NexGen Cyber Innovation and Technology Centre (NCITE) at its hub in Farnborough. There to meet us was John Plumb, NCITE UK Manager, who gave us a tour of the cyber lab while discussing the role of NCITE and how the Centre's work is becoming increasingly important in this network-centric age.

What is NCITE?

NCITE, previously known as Swift until a rebrand in January 2011, is part of Lockheed's Integrated Systems & Global Solutions (IS&GS) division, which focuses on three predominant sectors: Defence, Civil and National (also referred to as Security).

"When this Lab was set-up in 2006 it was really about showcasing what Lockheed had to offer but in 2009 we expanded to specifically undertake F-35 operational analysis," Plumb explained.

Since changing name to NCITE last year, the Centre has also altered its focus and its role is now evolving within the Lockheed Martin NextGen Innovation framework.

"Because we support the whole of Lockheed Martin UK we get to see everything. We've become a catalyst for horizontal integration," Plumb said. "We often bring parties together and we play a technology consultancy role by default."

The facility in Farnborough is home to over 200 Lockheed Martin employees, with around 15 of these dedicated to the NCITE lab.

....Excite at NCITE

We asked what NCITE did and about some of the activities it undertakes on a day-to-day basis.

"We host events and technology demonstrations; we have facilitated collaborative workshops, like MTDS (Mission Training via. Distributed Simulation) with NATO industry partners … and we provide facilities for other people to do training," Plumb explained. "We have a large data repository, which has for example intelligence reports, open source data, such as Jane's information, and full motion video which we generated using modelling and simulation tools.

"We also provide consultancy on project management and conduct rapid prototyping with scenario generation," Plumb added.

Elaborating on the bigger picture, Plumb said: "We're an IS&GS lab so we support IS&GS and their strategic thrust within the UK, Europe, the Middle East, and we've also undertaken some work for countries further East like India. Those strategic thrusts aren't just defence; our Civil division deals with air traffic control, the postal sorting, and it recently did the UK census for example."

Breaking it down, around 60% of NCITE's capabilities are directed towards R&D, with 30% being event hosting and the remaining 10% consultancy work. Focusing in on the main aspects that underpin NCITE's role, Plumb explained that collaboration and research and development (R&D) were the driving forces.

"The big thing about this place is collaboration, it's not just about using Lockheed Martin's expertise but it's also focused on bringing in partners and working with them to build customer solutions … that is one of the major thrusts for NexGen."

Emphasising the collaboration aspect, Plumb said that "We look for best-of-breed capabilities, if we don't have it we will get a partner who does.

"We aim to do joint R&D, that's the vision."

Plumb said that since becoming NCITE last year there was a "much greater emphasis on research and development now." However, the lab's role is again evolving as it seeks to integrate further into the supply chain.

"After concluding the R&D phase we tend to hand-over to deliver teams, although the CONOPS (Concept of Operations) that was revised at the end of last year for NexGen suggested that we should now grow our research and development to a higher state of maturity so that we may actually

go on to support the delivery. We haven't done it ourselves yet, but that is an important shift I think."

Shifting from Swift, to NCITE, and now looking ahead…

Discussing the future for NCITE UK, Plumb explained that "there's been a change in emphasis recently; cyber is really being driven heavily by IS&GS now." Also based in Farnborough is the UK Security Intelligence Centre (SIC), which is dedicated to the detection, identification and response to information security incidents. NCITE works in close collaboration with the SIC, which was only opened in December, to develop Lockheed Martin UK's cyber capabilities.

Last year was the year cyber threats suddenly became very real, with Lockheed joining a long list of other corporations like Sony, Booz Allen Hamilton and RSA to have been targeted by hacking groups like LulzSec and Anonymous. Plumb was reluctant to go into the details of the incident but it is clearly playing a formative part of the company's drive for cyber hygiene. Part of NCITE UK's role is to help develop these cyber capabilities in collaboration with other labs and IRAD.

At the opening of the UK SIC Giri Sivanesan, Lockheed Martin UK Head of Cyber, said: "In the future we will be looking to support more customers in the public and private sector through advanced cyber defence solutions and training customer staff in the latest cyber tradecraft."

Aside from cyber, Plumb talked through a number of other initiatives that NCITE UK is looking at in the future.

"The other thing that we want to do more of is replicating communication links, for example modelling tactical data link protocols and modelling bandwidth constraints so that you can stress the system to see where the choke points are. They are real-world issues. We're hoping to get more capability in to do just that."

Much of the work NCITE is involved with centres around aerospace applications, but Plumb and Simon Russell, NCITE UK's Chief Engineer, were quick to underline the significance of NCITE's work across the defence spectrum as it becomes increasingly net-centric.

"The demand for data and information exchange is going up. In the future customers will need to put in the requisite measures to actually ensure that they can mange that information exchange, that it increases and still be secure, which is quite a big challenge across the land, sea, maritime and space domains."