Defence and security in the cyber domain

Cyber defence: Support for national security imperatives

"We all recognise that in today's world living in an information age where so much of our communication, our economy, our virtual lives rest upon security of our information networks, that this is a very important area and indeed that it is treated as one of the priority areas by the cluster." *(Deputy Minister of Justice and Constitutional Development, Andries Nel, at a Justice, Crime Prevention and Security cluster media briefing, February 2011)*

Arguably one of the greatest threats to personal, national and international security, cyber-conflict has also become part of modern-day warfare. The interconnection of communications systems in cyberspace is the backbone of the information exchange that integrates and synchronises national infrastructure in most countries in the world today. A backbone that is critical to the economy and national security of a country.

Therefore, while there is great benefit from fast connectivity and vastly increased data storage space of Internet broadband, it has also increased exposure to the threat of cyber-attack – an attack that could delete personal wealth, disrupt economies, destroy critical infrastructure or affect military capability.

Cyber weapons – mostly malicious software launched through computers – are being described as weapons of mass disruption for individuals in society, businesses, governments and countries alike.

Originally designed for communication between researchers, the Internet has become a global tool with a proliferation of devices, from laptops to smartphones, connecting to it. This means that cyberspace – all the parts of the World Wide Web – has become virtually uncontrollable.

In the early 2000s, George W. Bush, President of the United States at the time, referred to cyberspace as the 'nervous system' of the nation's critical infrastructure. Some years later during the launch of the United Kingdom Cyber Strategy in 2009, then Prime Minister Gordon Brown, referred to cyber security as the *"21st century equivalent of securing the seas in the 19th century and the air in the 20th century."*

The nature and level of cyber-attacks are constantly changing. It is unclear when exactly experimental hacking became cyber vandalism, or when it became cyber-crime and finally cyber-warfare. It may have been during the Chinese hack attacks in May 2001 when vulnerability in Windows Internet Information Services was exploited to deface hundreds of US government websites. Perhaps it was the widespread use of custom Trojans in industrial espionage against the UK in 2003. The result was insight into the very real threat of cyber-conflict and the need to find ways to deal with it.

The rapid nature of cyber-attack and its ability to cross borders give military forces as well as terrorist groups the capability to launch attacks wherever they will, whether against military networks or critical infrastructure that depend on computer networks.

The impact of cyber-conflict can also be compounded when cyber-attacks are combined with conventional warfare, such as when Russia launched a cyber-attack on Georgia in 2008 and sent in 150 armoured tanks. This resulted in the US Department of Defence and the US government being tasked to urgently include the countering of cyber-attacks, surviving cyber-warfare and avoiding collateral damage under national security.

South Africa and cyber-defence

Despite an explosive growth in information and communications technology on the African continent in recent years, Internet penetration levels are still low with far less than 10% of more than the 2 billion people actively using the Internet. Although not as prevalent as elsewhere in the world, cyber-crime activities are affecting Africans who are increasingly falling prey to it propagators, such as online predators. Greater cyber security awareness and cyber-defence across the continent have become imperative.

In South Africa, cyber-defence is an important aspect of national security and the safekeeping of our constituency and resources. The country's incorporation into the global village in an attempt to bridge the digital divide has also increased its focus on cyber-security and cyber-defence. The rationale behind national cyber-defence is to counteract the threats posed by adversaries in cyberspace, which extend to all domains organisational, human, and financial to technological and information resources. Today, South Africa's cyber-safekeeping is guided by the *National Cyber-security Policy Framework for South Africa* developed by the Department of Communications.

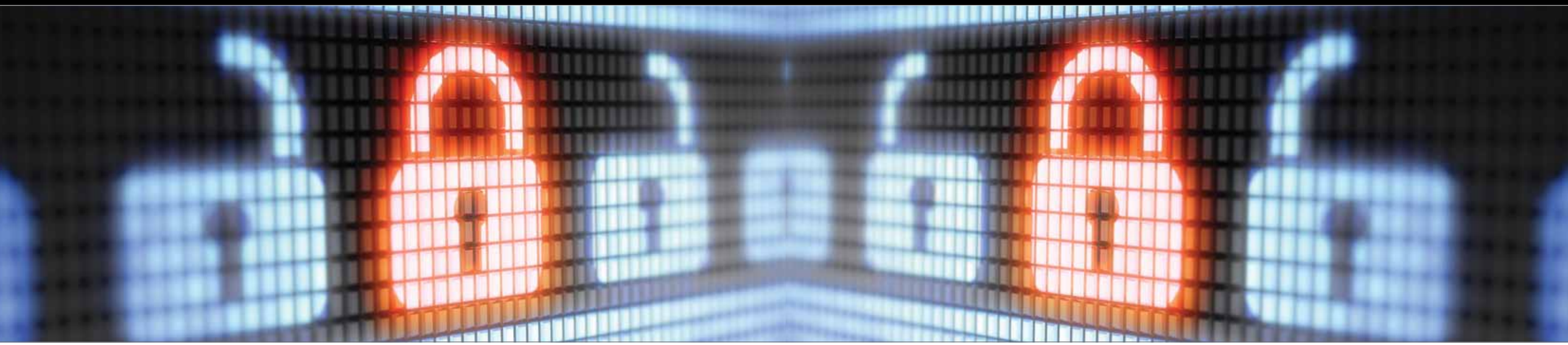
The role of the CSIR in South Africa's cyber-defence

Cyber research cannot be undertaken in isolation if it were to respond fully to the borderless reach of cyber-attack. The announcement to Parliament in February 2012 by the Minister of Justice that combatting cyber-crime would be a priority for 2012 followed in the wake of a decision by the Department of Communications in 2011 that it will *"boost cyber security [comes] in conjunction with the government's plans to battle crime using technology-based solutions and partnerships."*

The responsibility of securing our military cyberspace rests with the Directorate Information Warfare (DIW), which is mandated to continuously defend the information-based processes, information systems and communication networks of the military and destroy, neutralise and/or exploit the enemy's similar capabilities within the physical, information and cognitive domains in the event of war.

The CSIR's Cyber Defence Research Group supports the DIW in its endeavours with defence-related research and development. This includes continuously assessing the information battle space, identifying South Africa's vulnerabilities and adversary weaknesses and developing new defensive and offensive strategies and capabilities, as well as developing cyber security awareness material and helping vulnerable communities to become more cyber-aware. This supports a fierce commitment to providing cyber defence research, development and innovative solutions in support of national security imperatives.

DEFENCE AND SECURITY IN THE CYBER DOMAIN



Identifying network threats

Computer Networks are constantly under threat – be that from lone hackers or bored teenagers (known as "script kiddies") or organised criminal groups and foreign militaries.

Attackers have two technological advantages: firstly, the technological barrier against attacks is small and secondly, they benefit from safety of anonymity, especially when attacks are launched across borders.

Over the past few years, warfare in the cyber domain has commenced with Denial-of-Service attacks in Estonia, sabotage software that target Iran and state-sponsored industrial espionage. The sophistication of malware has increased from simple viruses and worms to highly sophisticated attack software. The CSIR's Cyber Defence Research Group is developing software for the detection of network attacks in their initial stages, before the attacker can achieve his or her goal.

Most network attacks use a standard methodology. The methodology consists of the following stages:

- **Target Identification:** The Target Identification phase represents actions undertaken by an attacker in choosing a target. This is typically done through web searches and looking at open directories.

- **Reconnaissance:** The Reconnaissance phase is when potential weak points are identified. These activities are the earliest indications that a network will fall under attack, before any real damage has occurred. For example, when scanning software is used – similar to how a criminal would 'case out' a physical target.

- **Attack stage:** The Attack phase sees the target system affected by the attacker with respect to confidentiality, integrity or availability. This stage comprises Ramp-up, Damage and Residue Stages. Even remotely controlled computers can be used in this process – referred to as "zombies" in a "botnet". One of the most popular damage actions is to deface web sites. This action can damage its target's system as well as its reputation. In the aftermath, signs of the attack can be seen in unintended communications and actions by malware after the attack. Typically, in a Denial-of-Service attack where millions of connections are used to overwhelm a target's ability to function, rouge connections are still made days after the actual attack.

- **Post-Attack Reconnaissance:** This occurs when the attackers revisit the crime scene in cyber space for scouting and other reconnaissance activities long after the attack.

The main types of network attacks have changed from the runaway viruses and worms of the 1990's to industrial espionage, sabotage and cyber warfare. These threats can only be guarded against by constant research into the technical aspects of network threats and possible countermeasures.

The CSIR's Cyber Defence Research Group focuses on identifying computer attacks in the Reconnaissance or Ramp-up stages in order to prevent an attacker from damaging the computer network. These stages are identified with the use of CSIR-developed network sensors. Different sensors are used, namely Access Sensors, Anomaly Sensors, Own-services Sensors, Scan-detection Sensors, and Targeted-information Sensors.

By integrating these sensors into a threat detection system, various network attack scenarios can be identified. Examples of network attack scenarios include industrial sabotage (such as the Stuxnet worm) and Web-defacement. These scenarios differ significantly from each other, and each requires detection through different network sensors.

The threat detection system integrates data from the network sensors into a temporal network attack model that maps possible attacks onto the various network attack scenarios. Network threats are simulated in a virtual environment, enabling the researcher to replay network attacks. By replaying network attacks, the network sensors can be optimised and updated in a safe environment without endangering other networks.

DEFENCE AND SECURITY IN THE CYBER DOMAIN

Seven psychological vulnerabilities of SEADM

Strong affect: trigger strong emotion in recipient to hamper decision-making ability;

Overloading: bombard recipient with a series of hurried persuasive axioms that calms and pacifies;

Reciprocation: presents and resolves a problem for recipient to extract an obligation to reciprocate

Deceptive relationship: builds relationship to extract information

Diffusion of responsibility and moral duty: convinces recipient that information disclosure is for the greater good and will hold no blame

Authority: portrays figure of authority linked to fear of punishment to solicit compliance and disclosure

Integrity and consistency: Individuals have an intrinsic desire to uphold their commitments, even if it were not their own.

Information security capability facilitates safe defence communication

The network security capability of the CSIR provides answers to the increasing need for secure networking in defence communications.

According to CSIR senior researcher, Erick Dube, his group – network security research – focuses its research on device authentication.

"Most people think that it is enough to just identify a computer-user and develop security around the user, while paying little or no attention to the device itself," he says. This, according to Dube is to the detriment of the users. This makes the network vulnerable to attacks by hackers. "The fact that you can identify the user is not adequate authentication for a device to access the network resources."

"Typically, the user is identified but we don't know the machine or device the user is using. This increases the likelihood of replay – when an unauthorised person gets hold of the password stored in the computer or device and makes use of them for nefarious reasons – such as injection."

Therefore, he adds, if we can identify the machine and/or the device as well as the user, we are able to reduce the risk.

In the defence environment, device authentication is critical. "It is critical in terms of the sensitivity of the information that the machine will have access to, once in the network," notes Dube. "Based on our in-house capability we are able to craft policies for the defence industry in line with the network device authentication."

"We can also develop and configure technologies that are applicable in device authentication for both local and international defence industries."

CSIR information security is suitably equipped to assist the defence industry with network intrusion detection and vulnerability assessment capabilities. This, in turn, will improve the safety of communication networks and enhance the security of the troops on the ground.

Attack detection in today's cyber-world

More often than not, the proponent of cyber-attack today is a skilled human manipulator, preying on human vulnerabilities by using various psychological triggers. For the unwary, these are difficult to identify, resist or counter and most cyber-attack victims are often simple, trusting individuals who do not expect an attack or even realise they had fallen prey to a social engineer.

CSIR researchers have used the two main perspectives of social engineering – the psychological and scientific (computer science) – in a Social Engineering Attack Detection Model (SEADM) to assist individuals to recognise, understand and counter social engineering attacks.

According to CSIR researcher, Francois Mouton, the psychological perspective focuses on emotions and cognitive abilities and the computer science perspective on information sensitivity, a cornerstone of information security. The model also incorporates factors such as urgency and understanding the request for information, as a successful defence requires the recognition and clear understanding of these triggers.

CSIR researchers identified seven psychological vulnerabilities that social engineers use as triggers on unsuspecting victims to develop the SEADM (see side-bar). Strong affect, for instance, is used in phishing attacks, where websites that masquerade as authentic sites to obtain confidential information illegally for financial gain are distributed via email. They create disparity between perception and truth and elicit a fear response. This compromises cognitive abilities and lessens the probability that the authenticity of the correspondence will be verified.

Social engineers use these triggers on unsuspecting victims to create a sense of discomfort. Attacks are launched on people in stressful work environments where decisions must be made instantaneously. Ideally we should recognise the triggers, but the reality is that human reasoning and decision-making are extremely complex and prone to error.

The CSIR's practical model can be easily implemented and used by all levels of employees. The SEADM is most effective when used in combination with training on various social engineering techniques, the psychological vulnerabilities it may elicit and institutional policies and procedures.

DEFENCE AND SECURITY IN THE CYBER DOMAIN

Cyber security awareness – Global Gaming

According to information sources, in Africa alone, more than 30 million cellphone users browse the internet in rural areas where there is little or no access to electricity. In fact, internationally, more than 500 million cellphone users do not have access to electricity. Many of these people charge their cellphones by using a car battery.

In deep rural areas, Internet banking via cellphones can save a day's travelling time to the closest town. However, the more people that have access to the internet, the greater the number who fall victim to cyber scams, cyber threats and cyber crime.

The CSIR's Cyber Defence Research Group has developed a Cyber Security Awareness (CSA) programme that serves as a 'self-defence' course for internet users. The project team started with the CSA project in 2009, in collaboration with the University of Venda. A two-pronged programme, the one part of the CSA programme comprises a community-based course in CSA, introduced to rural areas, consisting of 21 different cyber security related topics (the number of modules and the difficulty level vary depending on the target audience). This programme focuses on educating beginner internet and technology users in basic computer security for a number of target audiences. Secondly, the learning experience is supplemented by a range of CSA-themed games (both traditional board games and online games). The CSA programme is developed to balance traditional training methods with cyber security material and educational learning tools into a stimulating learning experience.

More than 60 trainers across South Africa have been equipped to present the courses in their communities and neighbourhoods, and more than 600 community members have already been trained. Packaged training sessions can also be offered at schools.

The range of games that form part of the CSA programme addresses the current need identified in beginner and novice computer users for basic cyber security practices, and emphasises the global nature of the internet by using both local and global components. It creates awareness in terms of the need for an anti-virus program, and re-enforces that computer worms, viruses and Trojans are negative, whilst an anti-virus program have a positive impact on a computer. Some of the benefits of playing the games include the education of current and future computer users on safe and secure online habits, increased awareness and understanding of the dangers of the internet, and the provision of the necessary knowledge to make the right decisions in internet-based situations. The games are designed to increase the players' knowledge about information security and cyber safety. The focus of all the games is educational entertainment, with a competitive component.

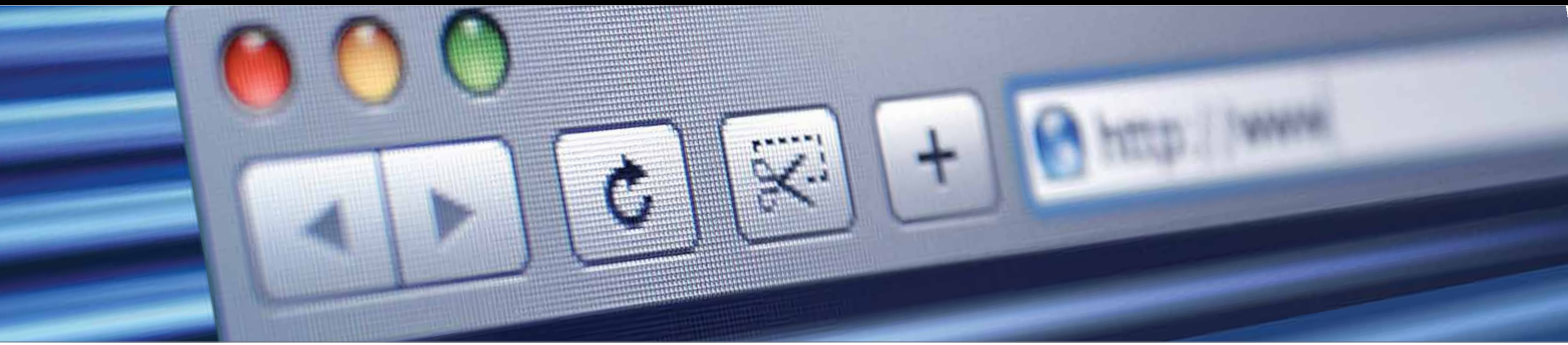
One of the games, Cyber Warrior Quest, provides a fun way to travel the virtual world whilst learning more about different CSA topics. The game can be played by individuals or teams. Players can only advance to a next level once his or her knowledge of a specific topic is deemed adequate. The game utilises Google Maps to show the progress of the competing players.

See the online area at **http://cyberawareness.co.za/race/race.php**

For a more South African flavour, the Siberytic game incorporated the principles of Stokvel to expose players to some of the hardware, software and other cyber-related components that they may encounter when using computers and the internet. The focus of the game is educational entertainment, with a competitive component.

Internet use in Africa: **http://www.sunny-people.com/about1.html**

DEFENCE AND SECURITY IN THE CYBER DOMAIN



Using an ontology for modelling the Information Sphere

A modern-day military environment receives an overwhelming amount of information from many different sources – all of which has to be processed, integrated, interpreted and exploited to gain situational awareness.

The integration of such heterogeneous information into a specific domain can only be done effectively when the domain is fully understood. Such understanding is the result of a process – from the initial understanding of the underlying concepts and meaning of the environment, which enables learning, drawing conclusions and making predictions to the development of a domain model on which reasoning processes can be based. Only then can successful information integration take place.

The CSIR's Cyber Defence Research Group is involved in a project to develop ontology with which to model the Information Sphere (IS). An ontology relates to the 'nature of being' and is a technology that enables a formal, shared representation of the key concepts of a specific domain and provides a way to attach meaning to the terms and relations used in describing the domain.

An ontology has been defined as *"a formal, explicit specification of a shared conceptualisation"*. It should, therefore, capture the domain from the point of view of a domain expert so that the information can be processed by computers and understood by humans.

Reasoning technologies enable us to reason about the facts contained in ontology. The Cyber Defence Research Group is collaborating with colleagues from the CSIR's Meraka institute's Knowledge Representation and Reasoning (KRR) group to benefit from their expertise in ontology construction, as well as the development of techniques to reason about ontology.

The use of ontologies in a variety of applications is growing rapidly and underlies the technology that drives the Semantic Web initiative. The latter is an endeavour by the World Wide Web Consortium (WC3) to promote standard data formats for web pages and add semantic content to web pages. Ontology is critical because it enables the representation of meaning which allows automated reasoning.

Ontologies provide a frame of reference for all stakeholders and facilitates the development of a common authoritative vocabulary set. It can also be used as a training tool for new entrants in the domain. In summary, ontology can be used as a tool to support the modelling and simulation of complex domains and other systems in the domain of interest.

While the definition of the IS ontology terminology was time consuming, the core part of the work was done during facilitated work sessions with domain experts. High-level IS entities and sub-categorisations were identified and refined. Formal descriptions of a domain have to be precise and commonly agreed upon, which require an iterative process.

The IS ontology has three core entities: *Human, Information and Information Infrastructure*. High-level concepts and relationships were implemented in the ontology. The Information Sphere ontology provides a framework for the development of lower level sub-domain ontologies. A number of these are under development.

The domain in which information operations, including offensive and defensive military information operations, take place is often described as the *Information Sphere*.

Allan & Gilbert (2010) defines it as *"The space of relationships among actors, information and information systems that form a sphere of interest and influence in or through which information-related activities, functions and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects."*

References

D.P. Allen & D.P. Gilbert, Qualifying the Information Sphere as a Domain. The Journal of Information Warfare, Vol. 9(3), 2010.

T. Grüber. A Translation Approach to Portable Ontology Specifications. Knowledge Acquisition, Vol 5, 1993.

DEFENCE AND SECURITY IN THE CYBER DOMAIN

The role of Social Engineering

Social engineering exploits human vulnerability by using various techniques to access information with which to bypass security systems.

People's basic 'good' nature makes them susceptible to social engineering techniques that activate psychological vulnerabilities and manipulate an individual to disclose the required information.

Facebook users (unknowingly) exposed: Social Engineering case in point

As social networking exploded around the world, communities have been created on platforms such as Facebook, Twitter and LinkedIn. People who frequent these sites generally do not realise the value of the information they divulge. They are even less aware of the tactics social engineers use to harvest the perceived 'worthless' profile data from social networking platforms or that these platforms have become a hunting ground for terrorist organisations to identify potential recruits or infiltrate critical infrastructure. The CSIR has undertaken research and experiments into this field to determine the extent to which people are exposed on these platforms and the likelihood of people allowing online approaches or recruitment by strangers.

Social media sites very effectively communicate the personalities of users. Social engineers convert the posts and comments from users on social news sites to text and use linguistic analysis software to identify the emotional dimensions, such as anger words and positive and negative emotions. Writing styles, language and function words provide insight into people's honesty, stability and self-image and identify their social relationships, emotions and thinking styles to help them determine their personalities.

These can determine personality traits and even gender, as men, for example, tend to use more articles (for example "a", "the"), nouns, prepositions, numbers, words per sentence and swear words than women. Men are also more likely to disclose political views and social engineers, always on the look-out, use this information as emotional triggers or to build trust with their targets.

Negativity and anger are two emotional states most often used during a social engineering attack, as anger affects the user's ability to think rationally and make logical decisions. Users on social networking sites who are prone to anger could identify themselves to social engineers on the prowl by repeatedly using negative words.

Social engineers have also bought into using 'The Big Five' of personality traits – openness, extraversion, conscientiousness, agreeableness and neuroticism – to profile their targets. Neurotic people, for instance, are easily stressed and upset – a trait that social engineers exploit with ease.

It is evident that many users do not understand or use the privacy control measures on social networking sites such as Facebook, where these measures are constantly updated. Users who make the list of their friends public, are also more prone to 'evil twin attacks' from social engineers who use rogue profiles that impersonate legitimate profiles to make friend requests. Often users implicitly trust profiles as they appear like legitimate people. Victims trust the familiarity of the 'friend' and provide information, such as the name and photograph of a trusted friend.

Such naïve users with a false sense of security are especially exposed to the nefarious intent of social engineers.
As such platforms are not only used by individuals but also by companies, the opportunities for information leakages and falling prey to cyber attacks have become a business and information security risk as well.