The latest version of this document supersedes all other previous issues.

Copyright © 2014 by CSC Australia Pty Ltd. ABN: 18 008 476 944 All Rights Reserved.

This document contains information that is the subject of copyright owned by or licensed to CSC Australia Pty Limited (CSC). The contents of this document shall not be used, copied or disclosed, other than for CSC purposes, without the prior written consent of CSC.

Disclaimer

CSC Australia Pty Limited (CSC) conducted this Threat Analysis and Risk Assessment as at November 2013 to update and enhance NSWEC’s electronic voting system (iVote). Whilst CSC has used all reasonable endeavours to assess the threats and risks associated with the in scope solution, based on available information, CSC does not warrant that all threats and risks have been identified or assessed.

CSC does not warrant or represent that the document is free from error or omissions and does not accept liability for any errors or omissions. To the extent that any express or implied guarantee or warranty as to condition, fitness, merchantability or suitability of this document for any particular purpose implied by law may be excluded, it is hereby expressly excluded and the liability of CSC for direct or consequential loss or damage is limited at CSC’s option to the re-supply of the document or the cost of correcting the document. In no event shall the responses to questions or any other information contained in this document be deemed to be incorporated into any contract or legal agreement under any circumstances without the express written consent of an officer of CSC.
Executive Summary

The NSW Electoral Commission (NSWEC) use of electronic voting in the form of the iVote application has and will continue to draw national and international attention as one of the leading electoral bodies to use the technology for voting in such a manner. With such coverage threat actors will be drawn to NSWEC's iVote as a means to achieve their individual goals whether directly related to the election, an attack against the Australian government or as a platform for media attention.

CSC has assessed the main threat actors that pose a potential risk to the NSW State Government Election 2015 and iVote due to their historical actions, current capability and possible motives. The main threat actors have a broad spectrum of capability that could threaten the use of iVote demonstrated by historical events to conduct offensive actions. Using the threat actor's capability and applying the generated attack trees for iVote, CSC and NSWEC staff conducted a tabletop exercise where NSWEC demonstrated controls that are either in place or will be in place to mitigate attacks.

The analysis from the tabletop exercise was then correlated with the threat actor’s capability to produce a number of recommendations and mitigations. Importantly, this can assist NSWEC during the early stages of the software development for iVote to ensure that the additional security controls are included at the design stage and not as late additions which can be costly or not feasible.

The following are a summary of the core recommendations which are detailed within the report:

- Protection of the application and system during development against any malicious code.
- Ensure the integrity of the audit logging systems by testing expected outputs, correlation and time stamps.
- Establish strong DDoS protection and countermeasures.
- Implement additional security controls on the registration system and associated database.
- Conduct security awareness training of staff, contractors and voters.
- Continued and accelerated threat actor monitoring leading up the SGE 2015 for any changes in capability, intent or triggers that may be a catalyst for an attack.

Not all controls and recommendations are strictly a technology solution. To assist in providing defence in depth, wider security controls are included as well as an intelligence collection plan to provide focus on key indicators that may precede a type of attack.

This is not a formal risk assessment. CSC has included as part of the final phase a risk assessment of the system once it is detailed - this will overlay the findings of this threat analysis report to the developed environment.
Introduction

Navigating this assessment

This threat analysis assessment was conducted using a systematic and logical framework. This overview of the sequence will assist readers in navigating and understanding the document:

1. **Assessment of Threat Actors** – provides a hierarchical breakdown, capability, profile summaries and attributes.
2. **Attack trees** – are developed specifically for the NSW State Government Election (SGE) 2015 system. These are independent of the threat actors.
3. **Threat Actor Capability Matrix** – provides a correlation between the threat actor’s capability and the attack trees.
4. **Ecosystem Analysis** – analyses the current and future environment and the factors that will affect attacks, threat actors and the NSW SGE 2015.
5. **Table top exercise** – the previous four steps culminated in a “wargame” with the NSWEC staff and CSC to walk through the attacks and effects on the ecosystem to discover any exposures.
6. **Threat Courses of Action** – the scorecard from the tabletop exercise is analysed in association with the threat actors to produce likely courses of action that could result in a successful attack, along with associated products to assist in mitigation.
7. **Recommendations** - the final section synthesises the analysis into tangible recommendations for the NSW SGE 2015.

Framework

CSC Cybersecurity has been engaged by NSWEC to update and enhance NSWEC’s electronic voting system (iVote) using CSC’s Threat Analysis and Risk Assessment methodology.

The Strategic Threat Assessment is the initial component of CSC’s Cybersecurity provisioning for an event and performs a key part of the overall framework. CSC also provides the other components as outlined below:
Objectives

The aim for the overall engagement is to:

- Understand the major threat actors which threaten iVote for the NSW SGE 2015, and map the relevant attack trees used by those actors;
- Identify any exposures that might exist from an examination of those attack trees; and
- Comprehensively document this exercise to satisfy future audit and external review.
Scope

The engagement is executed in four phases:

- Phase 1A – Threat Analysis Attack Tree
- Phase 1B – Course of Action and Threat Analysis Report
- Phase 2 – Security Risk Assessment
- Phase 3 – Ongoing Threat Review and consulting

This document is the conclusion of Phase 1A and 1B which is the end product for these two phases of this engagement. Phase 2 will commence once the NSWEC iVote system is specified with the awarded third party contractor which will allow for the overlay of the threat attack vectors with the actual system intended to be in place for SGE 2015.

On the basis of the systems architecture and implementation procedures proposed in the iVote strategy document, undertake an initial analysis of threats and risks associated with provision of iVote services for SGE 2015, including both the proposed iVote technical platform and procedures associated with operations for SGE 2015, using an attack tree approach.

- Pre-Task – CSC and NSWEC workshop - to clearly define communication, deliverables (in particular task 7) and initial information gathering.
- Task 1 – iVote Analysis - Analyse the iVote application from a technical and socio-political context to establish the major threat actors who are a source of risk to the NSWEC, the users of iVote and the wider public of NSW.
- Task 2 – Research Threat Actors - Research and analyse the identified threat actors to establish their motivation, capability, modus operandi and likely future actions.
- Task 3a – Mapping Threat Actor Matrix - Map the threat actors to a series of likely attack tree scenarios.
- Task 4a – Attack Tree Development - Create attack trees for each identified scenario.
- Task 4b – Attack Tree Development - Update attack trees for each identified scenario and course of action.
- Task 5 – Exposure Register - Produce a register of exposures identified by the attack trees
- Task 6 – Evaluation/Test Exposure Development - Provide control test criteria for each identified exposure in order for that to be later mapped to existing NSWEC security controls.
- Task 7 – Executive Summary & Recommendations - Produce a Threat Intelligence Estimate executive report based on outcomes of analysis, recommendations for further specific actions and any required ongoing programs of work. Additional reports based on agreement in workshop during initial kick-off workshop.
**Assumptions**

The following assumptions have been made for this assessment:

- CSC has analysed only the major threat actors to NSW iVote application for the SGE 2015 and has not included all global threat actors.
- Threat actors included are of known relevance at the date of this report. CSC recommends periodic reviews leading up to SGE 2015.
- This analysis only covers threat actors with intent to do a malicious action against NSW SGE 2015 and does not cover attacks resulting from error or omission.
Contents
Executive Summary ........................................................................................................... 2
Introduction ....................................................................................................................... 3
Navigating this assessment ............................................................................................. 3
Framework ....................................................................................................................... 3
Objectives ....................................................................................................................... 4
Scope ............................................................................................................................... 5
Assumptions .................................................................................................................... 6
Threat Actor Hierarchy ................................................................................................... 9
Threat Actor Profiles .................................................................................................... 10
Absentee Voters ............................................................................................................. 11
Al-Qaeda (AQ) ................................................................................................................ 12
Anonymous ................................................................................................................... 13
Anti-Coal / Mining Lobby ............................................................................................... 15
China ............................................................................................................................. 16
Domestic Organised Crime (DOC) ................................................................................ 18
Eastern European Organised Crime (EEOC) ................................................................. 19
Election Officials .......................................................................................................... 20
Internet Voting Hackers (IVH) ..................................................................................... 21
Iran ................................................................................................................................. 22
Jemaah Islamiyah (JI) .................................................................................................. 23
North Korea .................................................................................................................. 24
Opportunistic Hackers (OH) ......................................................................................... 25
Other Organised Crime (OOC) ...................................................................................... 26
Other Insiders ................................................................................................................ 27
Refugee Advocates ....................................................................................................... 28
Rogue Political Operatives (RPO) ................................................................................ 29
Syrian Electronic (SEA) ............................................................................................... 30
System Administrators ................................................................................................. 32
Threat Actor Attribution Matrix .................................................................................. 33
Tabletop exercise .......................................................................................................... 35
Threat Courses of Action .............................................................................................. 36
Combined Threat Capability and Exposures .................................................................. 36
Most likely courses of action ....................................................................................... 36
Figure 1 - Threat Actor Hierarchy
Threat Actor Profiles

The threat actor profiles are descriptions of current activities and incidents as well as background information about agents relevant for the NSW SGE 2015. They provide a high level overview of the threat actor including activities to date, typical targets, an overall evaluation and specific NSW SGE 2015 evaluation.

CSC has also provided a summary of threat actor attributes in each of the profiles which are later mapped to a reference table (Threat Actor Attribute Matrix) to visualise and weight attack attributes. The definitions for the attributes can be found in Appendix B.

Note: The information is largely based on open source research due to the intended potential of release in the public domain.
Absentee Voters

Access: Internal
Intention: Advantage, Harm
Boundary: Internal code
Organisation: Individual
Proficiency: Basic
Purpose: Manipulate, Steal
Attribution: Clandestine
Affiliations: NA

Date revised: 10 Jan 14

Summary: An absentee voter describes an individual with a disability or other reason that makes them unable to vote in person. Voters are granted access to the voting system to enable them to vote. Each voter would submit registration information, obtain the proper ballot given their registration status and then cast a single ballot.

Activity: Multiple voting has been an issue in the past with paper-based voting systems, usually through the voter either registering multiple times or registering when they are not actually eligible to vote. In the 1996 Australian election, a Divisional Returning Officer reported he had discovered 217 individuals in his electorate that were not actually eligible to vote who did, in fact, cast a vote. This may have been due to enrolled addresses being vacant land or too many people registered as living at the same address. There are also examples where impersonation has allowed for multiple votes. In the 2010 Australian election, a family was alleged to have voted more than 150 times by impersonating others, as you do not have to show ID when voting. The motive for this family was not stated in the media, but they were most likely wanting to push a particular party into power.

Target: Voters do not seek to manipulate votes, but they may be influenced, bullied or pressured by external sources. Voting for others, as was alleged in the Estonian election where elderly people voted who didn’t even own a computer. Elderly members were asked if they would vote and back a particular member. One elderly member said she did give her consent for voting. It was suspected that fictitious email addresses were created in the name of the elderly members in order to obtain username and passwords, which were then used to cast the e-ballots.

Those with intention for manipulation could gain further access by elevating their privileges. They could access files, folders or application data that the user was not initially granted access to. They could then install Trojans and backdoors to allow for further reconnaissance. In this case, it would be easy to manipulate the votes or get access to confidential information.

Overall Evaluation: Voters may, for example, attempt to use or expand their authorised level of access to damage the election system, change the results of the election or harm the credibility of the election results. They may also try to vote multiple times or manipulate the votes of others.

NSW SGE 2015 Evaluation: Voters using iVote would unlikely pose an increased threat to the SGE 2015. Manipulation such as outsider influence or vote buying could occur with the current postal voting system, but as for the ability to elevate privileges, the voter would have only limited access to the system. As such, they would need to have adept, specialist skills to achieve further access.
Al-Qaeda (AQ)

Access: External
Intention: Loss
Boundary: Religious
Organisation: Formal organisational
Proficiency: Intermediate
Purpose: Damage, Denial, Destruction, Steal
Attribution: Overt
Affiliations: Al-Qaeda Electronic Army (AQEA), Tunisian Cyber Army (TCA), Chinese Criminal elements, TeaMp0isoN, ZCompany Hacking Crew, Mujahideen Hacking Unit, 0xOmar, Jamaat-e-Islami, the Taliban

Date revised: 10 Jan 14

Summary: AQ is a global militant Islamist organisation founded by Osama bin Laden in Pakistan. Seized assets have shown intent to grow an organic cyber warfare capability and AQ operatives have undergoing advanced hacking training.64 AQ has published propaganda stating its intentions and promotion for a Cyber Jihad against the US critical infrastructure as early as 2010.4 This resulted in the creation of the AQEA and has lead to attacks against US and western government targets with support from other aligned groups."xv

Activity: Joint attacks with the TCA and AQEA under the banner of “Operation Black Summer” have included the Pentagon, US Customs and Border Protection and office of Personnel Management (extraction of information from an SQL database)xvi, US Bankxvii and well as two US petroleum companiesxviii. Operation Black Summer was a plan to breach the security of US websites - DDOS attacks. Other Jihadist attacks from affiliated groups have include UK government agencies, Israel Stock Exchange (DDOS), Israeli banks, credit card theft, and low level website defacements.xix Recently, AQ is reportedly linked to phone hacking scams targeting the US, with the aim of fund raising.xvi

Target: The targets will continue to be large western countries with particular focus on the US and UK. Other targets such as Australia will mainly be in response to Australia’s political or active involvement against extremist Islamic strongholds (being countries or areas the extremist Islamic community for an Islamic state).

Overall Evaluation AQ poses an emerging threat as it has shown interest in growing its cyber capability and has demonstrated this through attacks it has conducted. In addition, with AQ advanced human operative capability through indoctrination, subversion and then infiltration of sleeper cells it provides AQ with capability to potentially acquire direct access to systems other groups would dream about. AQ have shown that they continue to challenge the status quo for terrorist events and not much can be ruled out if cyber can be exploited to cause (directly or indirectly) mass causalities.

In addition, AQ have shown progressive refinement in their modus operandi coupled with an increasing ambition from young Jihadists who see cyber warfare as a new, efficient and relatively easy way to fight for propaganda of radical Islam worldwidexviii.

NSW SGE 2015 Evaluation: It is unlikely any direct threat will emerge due to the relative new capability, the winding down of Australian national political involvement in Islamic international affairs (such as forces leaving Afghanistan by the end of 2013) and the perceived low key international visibility of SGE 2015. Key indicators would be political events linked to the threats against Islamic coinciding with key election dates. The SGE 2015 could then be seen as a potential target for mass disruption to directly attack the western way of life, confidence in the government or systems.
Anonymous

Access: External
Intention: Harm, Embarrassment
Boundary: None
Organisation: Informal organisation
Proficiency: Advanced
Purpose: Indifferent
Attribution: Overt
Affiliations: TCA

Date Revised: 10 Jan 14

Summary: Anonymous can be considered a large, amorphous group of hackers responsible for some of the most publicised and large-scale cyber-attacks of the 21st century. Generally considered ‘hacktivists’, Anonymous widely uses its influence as a form of protest. The group has strongly opposed censorship issues and takes a moral stance on cyber-centric issues and rights, often with a physical presence attached to its online protests. The group’s effectiveness has been brought into question given their reliance on DDoS attacks and can be considered the most prominent internet vigilante group of modern times.

Activity: Drawing from a large, international pool of resources, the group typically organises operations from independent Internet relay channels, utilising a wide range of methods, including involuntary botnets to attack and/or procure secure information. From 2008 the group began a campaign of co-ordinated international hactivism, including attacks on major government agencies and global companies such as Paypal, Mastercard and Visa through sustained DDoS attacks.

In the Ohio 2012 election it was claimed they stopped voter fraud by putting up firewalls to stop the votes being manipulated. Although there is no proof this happened, it is plausible given past exploits.

In July 2012, Anonymous took at least 10 Australian government websites offline in a series of escalating attacks over proposed changes to privacy laws. In November, Anonymous posted a video criticising QLD Premier Campbell Newman over the state’s new anti-biking laws which resulted in harassing phone calls. In the same month, it was claimed that more than 170 Australian websites where hacked and DDoS attacks against AFP and the RBA occurred from an Anonymous group in Indonesia in relation to the Australian government spying allegations.

Target: Anonymous’ targets are varied, but include companies and organisations related to internet censorship, homophobia, child pornography, racism and drug distribution among others. In the past Anonymous has been responsible for significant down-time of major websites (FBI, Justice Department, Motion Picture Association of America, PayPal, etc.) and remains a major cyber security threat.

Overall Evaluation: Anonymous’ strength lies in its numbers and reach, allowing sustained attacks on high-priority targets. Anonymous’ main objective is disruption as a form of activism, but previous attacks suggest it is also proficient in obtaining classified and secure data, and physical theft. They use covert channels to avoid detection, even from major government bodies, though recent arrests and its failure to bring down targets have brought Anonymous’ current strength into question.

The decentralised nature of Anonymous makes identification and prosecution especially difficult, though dozens of purported members have been arrested in the last two years in countries including the US, UK and Australia.
Opinions on the group’s actual effectiveness vary substantially, though as a collective whole it has been shown to be resourceful, employing both legal and illegal means to achieve its goals.

**NSW SGE 2015 Evaluation**: NSWEC would only be a priority target of Anonymous if they perceive voter fraud occurring as in the Ohio case or the election breaches a personal liberty. They may also look at conducting a DDoS attack if they have an issue with the government or voting process.
Anti-Coal / Mining Lobby

Access: External
Intention: Advantage, Embarrassment
Boundary: International Law
Organisation: Informal organisation
Proficiency: Basic
Purpose: Damage, Manipulate
Attribution: Overt
Affiliations: NA

Date revised: 10 Jan 14

Summary: Anti-coal activists such as Quit Coal, Lock The Gate Alliance, and Flac support clean and renewable energy they protest against the use of new coal infrastructure and “dirty, old technology”. A mission statement released by activists lists protecting Australia’s natural, environmental and agricultural resources from “inappropriate mining”, as well as increasing public awareness of sustainable energy and food solutions.

Activity: In January 2013 an anti-coal activist used a laptop computer to draft a fake press release from the ANZ that listed its supposed withdrawal of support and funds for a proposed Whitehaven coal mine. The fake press release was published by various media outlets, but was later retracted. This resulted in a reverse pump and dump in which ANZ’s stock fell by nine percent ($314 million). The activist was a member of Flac, who had been camping out at the Whitehaven coal mine project in protest of the development. In another incident, activists placed 100 fake out-of-order signs on ANZ ATMs in order to cause disruption to the bank. The activists used social media to circulate the protest. The group has widely been reported as saying they are prepared to use unconventional and modern means of protest in order to push their agenda and reach the general public.

A protestors linked to anti-coal and climate change action was also brought into media attention in 2013 when he gained access to Tony Abbott’s election victory party at the Four Seasons Hotel using a fake wristband made from a Starburst wrapper. He was able to come into close proximity with Tony Abbott for more than a minute before being taken away by authorities. The protestor was trying to get Tony Abbott’s attention and asked him if he could be a representative for the Liberal Party for one of the Sydney regions.

Target: Anti-coal protestors generally target mining and coal companies directly or the companies involved in funding future projects they perceive will threaten the natural environment. Recent attacks against the ANZ bank were triggered following Greenpeace’s statement that the bank was the leading financial body of Australia’s coal industry. As exemplified by the recent Tony Abbott incident, protestors will get involved in a political manner if they feel it will help them in their cause.

Overall Evaluation: Until the ANZ faux press release scandal, anti-coal activists had generally not been known to employ electronic means of protest, but recent cyber-attacks suggest a growing level of proficiency. Although, largely non-physical and non-violent attacks, while limited to basic means of impersonation, have shown sophistication in spread and led to major disruption.

NSW SGE 2015 Evaluation: As the NSWEC is not directly involved in coal-industry policy or funding, the threat level from anti-coal activists remains low. However, they are elevating their protest in the political circles with hopes to influence the public to vote for left-wing groups and to motivate parties’ policies. This could lead to targeting of the SGE 2015.
China

Access: External
Intention: Advantage
Boundary: National Law
Organisation: Government
Proficiency: Advanced
Purpose: Manipulate, Steal
Attribution: Clandestine
Affiliations: North Korea
Other: Nil

Date revised: 10 Jan 14

Summary: China use cyber warfare as a means to achieve its national objectives. There are many individuals and groups acting out of China and for the purposes of this profile summary it includes the People’s Liberation Army (PLA)xxxii, Chinese Intelligence services, government sponsored independent and corporate actors.

To date a majority of the Chinese attacks have been focused on collecting information and intelligence – whether that is militaryxxxiv, government or economic related. China is a key international threat actor due to high level of activity, widespread targeting, systematic and prolonged attacks expended to acquire the target.

Activity: China has demonstrated it carries out well planned and executed activities that involve social engineering, hardware / code modification at time of creation, to international political manoeuvring to position itself as a greater cyber power (ie. United Nations). Recently, there have been limited disruptive or destructive attacks; however the level of access for collection purposes could easily be turned to affect such means.

Many cyber-attacks are speculated to originate from China, however there are some key known public events that demonstrate capability and motive to target Australia. Hackers obtained classified blueprints and cabling details of the new ASIO building in Canberra. Also Chinese owned Huawei was banned from bidding on the Australian National Broadband Network speculated due to ASIO security concerns with their routers in 2012.

There has been numerous espionage attacks claimed from Chinese groups (sponsored or not) where each countriesxxxv security services have notified business including, but not limited to: US, UK, Canada, Germany, Taiwan, Japan, India and Australia. Other attacks against prominent organisations such as NATO, Tibetan and Uygur groups are also documented. In addition, Chinese owned ZTE had security concerns raised over backdoors in it mobile phone productsxxxvi

Although no known direct electronic voting attacks have originated from China, attacks against the US Federal Election Commission occurred on 1 October, to which an investigation is underway.xxxvii

Target: Chinese hackers in recent years have begun to move beyond the archetypical procedures used by state-sponsored actors (such as the events described above) and into increasingly advanced operations against specialised targets and this trend is expected to continue exponentially. Modus operandi has included defeating secure authenticationxxxviii, bridging air gaps, targeting deployed military platforms (ships at sea), leveraging the cloud for command and control exploits, and compromising mobile devices through sophisticated malware.

Overall Evaluation: China will continue to exploit government, military, industrial, and non-governmental computer systems as long as it is within their national objectives, even under increased international pressure. The attacks will continue to be clandestine in nature with a focus on intelligence and information with any
individual attack difficult to attribute. China will continue with new research, development and investment to improve exploitation capabilities significantly. Lastly, the volume of attacks and widespread targeting will continue with its large personnel capability allowing China to reach most desired targets.

**NSW SGE 2015 Evaluation:** Although not consistent with National Policy, which to date have aligned with their public attacks, China could look to the election and internet voting in three different ways. Firstly, from information gathering point of view: NSWEC is one of the world leaders in adopting electronic voting and it presents a good information target on such systems for potential future exploitation. Secondly, China may attempt to influence the outcome of electronic voting for its national objective to secure global resources\(^{\text{xiii}}\), such as the limiting the National Part influence\(^{\text{xxxv}}\). Lastly, China could see this as a means to infiltrate and leave sleeper malware technology in the hope for future payoff.
Domestic Organised Crime (DOC)

**Access:** External

**Intention:** Advantage, Loss

**Boundary:** Internal code

**Organisation:** Formal organisation

**Proficiency:** Basic

**Purpose:** Manipulate, Steal

**Attribution:** Covert

**Affiliations:** NA

**Date revised:** 10 Jan 14

**Summary:** DOC organisations such as the Bikie Gangs, Ethnic Gangs and Commercial Drug Suppliers have a broad range of capabilities and functions. They are adept at utilising their people and resources to force change in order to achieve their goal; although little investment has been noted in a cyber capability. They are typically external but often can get access to insiders.

**Activity:** DOC organisation activity is very limited in the cyber domain with reported activities restricted to fraud and card skimming. However, these criminal organisations are well funded and do use technology on their internal operations, such as secure communications and encryption to thwart tradition policing efforts of eavesdropping. Other investment might include either converting or planting insider agents into government and private organisations; this has been seen in NSW where Police intelligence was compromised by an insider working for a Bikie gang involved in commercial illegal drug supply. Also recent cyber attacks against Queensland Police could be linked to domestic criminal organisations. There are ties between some DOC’s and local government and state government and DOC’s may play a role in some political organisations.

The Australian Crime Commission warned of a significant cyber crime threat from domestic organised crime along international criminal groups.

**Target:** DOC ethnic groups typically have strong links within particular ethnic communities and may use this to turn insiders to enact low level cyber criminal activities.

**Overall Evaluation:** This agent is external, but it uses organisational influence to change the playing field and leverage its contacts. Activity is largely opportunistic with business-driven, objective-oriented, and savvy participants who are good at hiding and gaining legal protection. No current information indicates a establishing a cyber capability as means of regular criminal activity for exploitation.

**NSW SGE 2015 Evaluation:** NSWEC would not be a priority target of DOC unless they were interested in influencing a political outcome and even then they are more likely to utilise non-cyber means for this purpose.
Eastern European Organised Crime (EEOC)

Access: External
Intention: Loss
Boundary: Internal code
Organisation: Formal organisation
Proficiency: Advanced
Purpose: Steal
Attribution: Covert
Affiliations: Russian Government

Date revised: 10 Jan 14

Summary: EEOC organisations have a broad range of capabilities and functions, and maybe publicly known organised crime groups such as Tambovskaya. They are adept at utilising their people and resources to force change in order to achieve their goal. For example, they are typically external but often can get access to insiders and other resources to drive changes facilitating even greater access.

Activity: EEOC activity has increased over the past ten years in the area of cybercrime. This rise has been well documented. The ease and relative anonymity of cybercrime especially suits the needs of these organisations, and they are constantly expanding their capabilities in this area. They are rapidly innovating new and unpredictable methods of operation. Most criminal organisations are well funded and see technology theft and cybercrime as lucrative and worth significant investment, reportedly $1.5 billion in payment card fraud in Europe alone. This investment usually includes either converting or planting insider agents into government and private organisations. In some areas of the world there are strong ties between organised crime and government. EEOC are often closely aligned with the security services in Eastern Europe and often recruit from them to gain specialised skills and influence.

Target: Western financial sector is a popular target for EEOC. Banking credentials are easily obtained, used for Internet fraud or resold on the black market – such as recently where the US indicted five hackers for $300m cybercrime spree. Other activities such as online pornography could enable the agent to blackmail employees with personal problems to provide assistance from the inside. Theft of personal identity information is a growing opportunity for this agent as well as use of ransom-ware to extort money from victim organisations and individuals.

Overall Evaluation: This agent is external, but it uses organisational influence to change the playing field and leverage its contacts. The agent can assert almost unlimited influence in procuring intellectual property and the sale or distribution of goods. Activity is largely opportunistic with business-driven, objective-oriented, and savvy participants who are good at hiding and gaining legal protection.

NSW SGE 2015 Evaluation: NSWEC would not be a priority target of EEOC unless they were hired by other threat actors for the purpose. EEOC have provided DDoS attacks, data collection and infrastructure for attacks for a number of other threat actors in the past for monetary gain. In particular nation state actors might use EEOC to achieve their aims to target NSWEC.
Election Officials

Access: Internal
Intention: Advantage
Boundary: Internal
Organisation: Individual
Proficiency: Basic
Purpose: Manipulate, Steal
Attribution: Clandestine
Affiliations: NA

Date revised: 10 Jan 14

Summary: Election officials are users of the election system with access to confidential voter and ballot information. They may have a significant level of access to data on voting system equipment.

Activity: In the 2011 Australian election, Pauline Hanson was sent a hoax email stating that 1200 votes had allegedly been put in the blank pile on purpose by an election official so the votes wouldn’t count. Hanson took the case to court but was ultimately unsuccessful, with various sources believing the act was initiated by an anti-voting fraud group who are convinced Australia’s voting system is corrupt. xlv xlvi

Clive Palmer, during the 2013 election, stated he believes election fraud occurs. He noted that voters do not have to produce IDs, votes are written in pencil (which can be altered) and ballots have not been validated (missing an election official’s initial, are included in the count). His party was also not invited to one of the recounts as a scrutineer. xlvii He also mentioned that if there are any questions in regards to voting fraud, the Court of Disputed Returns does not have access to examine the ballot papers. xlviii

Target: While election officials may be restricted from certain administrative functions, such as software installation, they often have relatively unrestricted physical access to voting system equipment. Election officials may also be involved in this voter interference, which provides perhaps the best venue for mass exploitation. xlix

Overall Evaluation Officials have control over most aspects of elections, including the count, ballot security and access for scrutineers. l Malicious election officials could use their position to exploit voting systems and influence voting.

NSW SGE 2015 Evaluation: Election officials would be a low threat to SGE 2015. With the iVote system officials would be restricted to only being able to access what is required for their particular job. The main threat would come from officials who work on the help desk whom interact directly with voters and would be able to influence their vote.
Internet Voting Hackers (IVH)

Access: External  
Intention: Embarrassment  
Boundary: None  
Organisation: Individual  
Proficiency: Advanced  
Purpose: Indifferent  
Attribution: Overt  
Affiliations: Other hacktivist groups including Anonymous

Date revised: 10 Jan 14

Summary: IVH individuals have a broad range of capabilities depending on individual skill level which varies significantly. They target Internet voting applications to demonstrate the lack of security, show their lack of trust in governments generally and to demonstrate their skill level to the rest of the hacker community. Their actions are very public and may be more about causing embarrassment than actually impacting Internet voting applications or the results of elections.

Activity: IVH individuals wish to bring attention to the inadequate security used in electronic voting systems and may be associated with anti-internet voting organisations. In July 2011 a hacker using the handle Abhaxas (icon used above) leaked via Pastebin a lengthy text file revealing part of Florida's voter database (voter statistics, candidates, and electoral race data). He stated in releasing the information: “So, this is a little ironic. Here is inside details of Florida voting systems. Now.. who still believes voting isn't rigged? If the United States Government can't even keep their ballot systems secure, why trust them at all? FAIL!”

After officials reported the system was secure following remediation, Abhaxas again gained access to private file directories publicising the subsequent insecurity. IVH may be motivated by a wish to emulate the lawful work of Internet voting security researchers such as Scott Wolchok from the University of Michigan, who breached the Washington DC election system in a test in 2010. Wolchok and his colleagues have received significant media attention for their exploits and IVH might choose replicate these activities in an illegal manner to gain notoriety and promote their cause.

Target: IVH specifically target Internet voting applications but may also be involved in other hacktivist activity such as criticising government restrictions and surveillance, promoting the freedom of information on the Internet and other popular causes within this sub-culture.

Overall Evaluation: This agent is external with a particular agenda against Internet voting however may be look for targets of opportunity given the limited resources they have available as an individual.

NSW SGE 2015 Evaluation: NSWEC would be a priority target of IVH given their opposition to internet voting and desire to demonstrate its insecurity. IVH individuals may take encouragement from the large Anti-Internet Voting Lobby that are prominent in publicising breaches of Internet voting systems including the activities of Scott Wolchok and his colleagues. IVH breaches are often reported in sensationalist language questioning the security of Internet voting without any analysis of the nature and impact of the actual attack i.e. “Voters concerned about the reliability of electronic voting may now have another reason to worry.”
Iran

Access: External
Intention: Advantage, Harm
Boundary: National law
Organisation: Government
Proficiency: Intermediate
Purpose: Destruction, Steal
Attribution: Clandestine
Affiliations: Cyber Hezbollah, Ashiyane, Basij, SEA, Islamic Cyber Resistance Group
Other: Nil

Date revised: 10 Jan 14

Summary: Currently Iran is widely assessed as a “Third Tier Cyber Power” in terms of capability. This shows clear intent and with the added support of third parties and a reported $1 billion investment in Cyber warfare capability, Iran poses a threat internationally. This is of particular military interest as Tehran’s has weak conventional forces, cyber-attacks could be an attractive alternative. It is expected that Iran would do more damage to public perceptions than actual infrastructure.

Iran’s cyber operations consist of the Iranian Revolutionary Guard Corps (IRGC) with political/criminal hacker group Ashiyane; and the Basij (cyber mercenaries). Although Iran is investing heavily to deepen and expand its organic cyber warfare capacity, this has taken a recent blow with the assassination of Mojtaba Ahmadi, who served as commander of the Cyber War Headquarters.

Activity: Iran has been accredited with cyber-attacks against US corporations including oil, gas and electricity companies, reportedly with the goal of sabotage rather than espionage - no official Iranian government acknowledgement. There is speculation of involvement in a number of hacking incidents including against Voice of America, and Dutch firm DigiNotar (security certificates). Iran has also worked with Hezbollah in a suspected August 2012 cyber-attacks on the state-owned oil company Saudi Aramco and on Qatari producer RasGas.

Most recently and significantly, Iran has reported attacked American financial institutions including Bank of America, PNC Financial Services Group, Sun Trust Banks Inc., and BB&T Corp (DDOS). The Izz ad-Din al-Qassam Cyber Fighters claim responsibility for all of these incidents.

Target: The attacks has largely been disruptive and destructive in nature and mainly targeted at Israel, Middle Eastern Israeli sympathisers, US and some European entities.

Overall Evaluation: Iran’s motive and intent is strong with a desire to strike back at the west and its allies for sanctions, assassinations and overall recognition as a power in the region. Iran’s organic capability is poor; however, it has strong ties with other third tier groups and higher capability through “hired guns”. The most likely and most damaging possibility is a campaign of attacks that creates a new political crisis. Iran desires an increased cyber capability with some assessments have Iran as being expected to be “edging in on the top tier” in five year’s time.

NSW SGE 2015 Evaluation: Iran poses minimal threat to the election due to the low political involvement by the Australian Federal government with the Iranian crisis and Australia’s minor international political influence in the Middle East. The threat could increase if Australia escalated its anti-Iran rhetoric and strongly and visibility supported any conventional action against Iran.
Jemaah Islamiyah (JI)

Access: External
Intention: Loss
Boundary: Religious
Organisation: Formal organisation
Proficiency: Basic
Purpose: Indifferent

Affiliations: AQ affiliated groups, Abu Sayaf Group (ASG), Jamaah Anshurat Tauhid (JAT), Front Pembela Islam (FPI), Majelis Mujahidin Indonesia (MMI), KOMPAK (Crisis Action Committee), Laskar Jundullah and Majelis Dakwah Umat Indonesia (MDUI), Moro Islamic Liberation Front (MILF).

Other: Nil

Date revised: 10 Jan 14

Summary: JI are listed with Australia, US, UK, New Zealand and the United Nations as a terrorist group. They are known for their spectacular physical attacks in Asia including the Bali bombing (2002), Jakarta Marriott Hotel bombing (2003) and bombing of the Australian embassy in Jakarta (2004). JI has been responsible for preparing, planning or assisting of terrorist attacks against a range of targets, but particularly Christian, western and regional governments’ interests in South-East Asia. Currently, JI is focusing on membership consolidation and rebuilding of its support networks, in alignment with their strategic plan which extends to 2025.

Activity: JI cyber capability is limited however it is associated with extremist websites namely, arrahmah.com, muslimdaily.net, Voa-Islam.com and al-tawbah.com. Arrahmah.com, muslimdaily.net and Voa-islam.com which include cyber warfare manuals. In 2011, Philippines and United States authorities arrested four members of a Filipino hackers group whose operation is linked to JI member Muhammad Zamir. In addition in 2012 the Philippine Criminal Investigation and Detection Group (CIDG) arrested a group of Filipino hackers at the payroll of terrorist group JI. Recently Australian Department of Foreign Affairs and Trade issued warning for Australians travelling to the 2012 Christmas period that “terrorists have previously attacked or planned to attack places where Westerners gather.”

Target: JI will continue to use whatever means are at its disposal to further its cause to establish south east Asian Islamic states with particular focus in Indonesia and that of regional western power Australia.

Overall Evaluation: JI have shown clear capability, motive and intent to direct cause damage to Australia and western interests within South East Asia. Although they have aimed for devastating events to date, they may use cyber as a means to achieve that end state.

NSW SGE 2015 Evaluation: JI is highly unlikely to have the election as a potential target as it would not fit within their historical modus operandi of physical spectacular events.
North Korea

Access: External
Intention: Harm
Boundary: National law
Organisation: Government
Proficiency: Intermediate
Purpose: Damage, Denial, Destruction
Attribution: Covert
Affiliations: China\textsuperscript{lxiv}, Iran, Syria
Other: Nil

Date revised: 10 Jan 14

Summary: The North Korean government focuses on its region and national sovereignty, however, due to the erratic nature its leadership and historical actions it is considered a wider international threat actor. North Korea’s cyber capability is relatively unknown and unproven due to the secretive nature of the regime, however, South Korean and US officials report large investment, dedicated teams and a rapidly increasing highly skilled capability. It has potential links or alignment with China due to proximity and strong political ties as well as dealings with Syria and Iran; placing it nicely with other regimes with strong cyber capabilities.

Activity: North Korea’s leader Kim Jong-un is openly confident in North Korea’s cyber capabilities against South Korea. North Korea reportedly operates a dedicated cyber team under the Reconnaissance General Bureau of the Korean People’s Army, with reports of up to 3,000 hackers that largely operate in a clandestine manner. It has been reported that North Korean hackers work under cover for various software companies and trading firms in China, Southeast Asia and Europe\textsuperscript{lxv} which would be consistent with the bold foreign intelligence moves by the erratic state.

The nation has been implicated in cyber-attacks ranging from computer network exploitation to distributed DoS attacks\textsuperscript{lxvi} and in some assessments North Korea’s cyber capabilities were behind only those of the United States and Russia\textsuperscript{lxvii}. There are also suspicions of North Korea attacks against targeted South Korean banks and media companies an attempt to steal highly classified intelligence on defence and security (a sophisticated malware attack wiping hard drives and ATM services). Recent reports that North Korea has again injected malware into computer games to infect South Korean computers this was extremely successful against a major airport.\textsuperscript{lxviii}

Target: North Korea’s targets have traditionally been South Korea and its main international supporter the US. That said the regime will likely target anyone who engages them as political adversary, regime degradation or perceived aggressive behaviour to threaten the nation state.

Overall Evaluation: North Korea has demonstrated cyber capability through its actions, traceable events and the poetical statements. Even though there are various reports around the size and skill of the capability, they would definitely be in the world’s top 10 cyber warfare. Of note is North Korea’s history of wild exploits that may translate into bold initiatives to inject personnel into IT roles to gain access to code or systems.

NSW SGE 2015 Evaluation: Australia is not perceived by North Korea as being actively aggressive towards its destabilisation and therefore unlikely to be on the radar for cyber-attacks. If Australian government foreign policy was to change towards aggressively pressuring North Korea around its nuclear ambitions (or other controversial North Korean initiatives) then the Australian government may become a target.
Opportunist Hackers (OH)

**Access:** External  
**Intention:** Harm  
**Boundary:** None  
**Organisation:** Individual  
**Proficiency:** Advanced  
**Purpose:** Indifferent  
**Attribution:** Overt  

**Affiliations:** Other OH individuals and hacking groups including Anonymous and Anti-Internet Voting Hacktivists

**Date revised:** 10 Jan 14

**Summary:** OH individuals have a broad range of capabilities depending on individual skill level. They are opportunistic and primarily interested in technical exploration and demonstrating their skill level to the rest of the hacker community. They are unlike Internet Voting Hackers whom target specifically iVote systems. Their actions are often public and may be more about showing their technical skills than causing impact.

**Activity:** OH individuals have long history on the Internet i.e Mafiaboy attacks on CNN, eBay, Amazon and others in 2000\(^{lxxix}\). Their techniques such as web defacement and Distributed Denial of Service (DDoS) attacks are often used by groups with a particular target in mind, but lack the technical capability for a highly targeted sophisticated attack i.e. Syrian Electronic Army.

In November 2013, it was claimed that a member of the Anonymous group in Indonesia hacked the Reserve Australia Bank (RBA) and Australian Federal Police (AFP) supposedly temporarily shutting them down. The RBA stated that they were subject to an attack but there was no outage and the AFP only had a short outage. Both the RBA and AFP stated that no sensitive information was accessed. The attack was due to the revelations that Australian was spying on the Indonesia’s president and wife.\(^{lxxx}\)

**Target:** OH individuals have no particular target but are looking for targets of opportunity for exploring and demonstrating their technical skills.

**Overall Evaluation:** This agent is external with no particular agenda and is largely opportunistic. They tend to have limited resources available as an individual but may collaborate with other OHs to divide tasks and gain skills.

**NSW SGE 2015 Evaluation:** NSWEC would not be a priority target of OH. However, if a vulnerability in iVote was found and circulated within the hacker community they may choose to take advantage of it.
Other Organised Crime (OOC)

Access: External
Intention: Loss
Boundary: Internal code
Organisation: Formal organisation
Proficiency: Intermediate
Purpose: Steal
Attribution: Covert
Affiliations: NA

Date revised: 10 Jan 14

Summary: Cybercrime acts require a high degree of organisation and specialisation. It is likely that the level of involvement of conventional organised criminal groups in cybercrime is high in particular financial-driven cybercrime acts such as computer-related fraud, forgery and identity offences. OOC organisations such as the Cosa Nostra, Yakuza and Chinese Triads have a broad range of capabilities and functions. They are adept at utilising their people and resources to force change in order to achieve their goal. They are typically external but often can get access to insiders.

Activity: Is limited in the cyber domain although niche players such as Brazilian and Chinese cyber groups have had impact within their home country and regional area. These crime organisations are well funded and use technology on their internal operations. They are entrepreneurial and invest in new areas to exploit opportunity. For instance a number of them are heavily involved with online gambling globally including the Cosa Nostra. Other methods might include either converting or planting insider agents into government and private organizations to achieve their aims. In some areas of the world there are strong ties between OOC and local, state and federal government.

There is also increasing concern about the scale of cyber victims in Eastern Asia, which leads to a possible significant role for domestic crime groups.

Target: Activities such as online gambling could enable the agent to blackmail employees with personal problems to provide assistance from the inside. OOC plan, organise and commit all forms of online crime – from fraud, theft and extortion, to the abuse of children. OOC also typically also have strong links within particular ethnic communities and may use this to turn insiders.

Evaluation Considerations: This agent is external, but it uses organisational influence to change the playing field and leverage its contacts. Activity is largely opportunistic with business-driven, objective-oriented, and savvy participants who are good at hiding and gaining legal protection.

NSW SGE 2015 Evaluation: NSWEC would not be a priority target of OOC unless they were interested in influencing a political outcome and even then they are more likely to utilise non-cyber means. It is possible that OOC may also be used by other threat actors to hire their skills for monetary exchange.
Other Insiders

**Access:** Internal

**Intention:** Advantage, Embarrassment

**Boundary:** Internal code

**Organisation:** Individual

**Proficiency:** Intermediate

**Purpose:** Damage, Destruction, Manipulate

**Attribution:** Clandestine

**Affiliations:** Potential foreign governments or organised crime

---

**Date revised:** 10 Jan 14

**Summary:** Other insiders could be any other individuals or organisations that may have privileged access to voting system equipment, either before, during or after an election is conducted. This could include voting system manufacturers and voting system integrators. It would include anyone who doesn’t work directly for the election or have privileged access to the system.

**Activity:** Manufacturers have been accused of altering their products before handing them over to clients. Chinese-owned Huawei was banned from bidding on the Australian National Broadband Network due to speculated ASIO security concerns with their routers in 2012. Although it was never proven Huawei had maliciously changed any of its network devices in the past, the Australian government was concerned with Chinese cyber-attacks through the networking hardware due to previous linked events between Huawei and the Chinese.

It was also claimed Lenovo computers that were manufactured in China had built in ‘malicious circuits’ and vulnerabilities in the firmware. They were banned by many countries’ government agencies due to the secret nature of their work.

**Target:** An insider would probably aim to manipulate or disrupt the system in a covert manner. When someone who has permission to access a system or network misuses that access to attack the network or steal data, major disruption could follow. They could also manipulate the system prior to it being implemented to allow for future, backdoor access to the system. Insider attacks can be difficult to trace because most security measures are designed to protect against outside attacks and insiders can know how to avoid them. They can also happen by accident when a network isn't properly secured, ie. someone can stumble across data they shouldn't be allowed to access.

**Overall Evaluation:** Insiders pose a significant security risk to businesses. They can undertake fraud, sabotage, privacy breaches and intellectual property theft are more legitimate given their level of access and privileges. Their knowledge of business functions and company protocol also allows them to work more covertly than outsiders. The threat becomes even greater if there is collusion amongst insiders or security controls are tampered with.

**NSW SGE 2015 Evaluation:** An insider will always pose a high risk as they have direct access to the iVote system. Whether they are the threat or as an actor for another, they would have the ability to manipulate or disrupt the iVote system with little trace. Manufacturers could alter devices before selling them to NSWEC and could put a ‘backdoor’ in the device they could use at a later date.
Refugee Advocates

Access: External
Intention: Advantage, Embarrassment
Boundary: International law
Organisation: Informal organisation
Proficiency: Basic
Purpose: Damage, Manipulate
Attribution: Overt
Affiliations: NA

Date revised: 10 Jan 14

Summary: Refugee groups protest for the rights of refugees and are opposed to mandatory detention and offshore processing. They typically protest through organised public rallies, public forums and aim to get these events reported in the media.

Activity: One of the main refugee protest groups is the Refugee Action Coalition (RAC), which protests widely, with seven members arrested for trying to communicate with refugees in detention in 2012 after trouble with police. An English teacher (working two days a week for the NSW Teachers Federation as a multicultural affairs officer) was also brought under attention after he was caught heckling opposition immigration spokesman Scott Morrison while on federation time. He was among a group protesting the decision to return detainee Seena Akhlaqi Sheikhdost, whose parents died in the Christmas Island boat disaster.

There has been no cyber activity recorded to date by any refugee activist groups.

Target: Refugee groups seek to promote their views to the public and target politicians on issues relating to the rights of asylum seekers, refugees and mandatory detention, the latter of which they label "mental illness factories". They have made public the fact they are prepared to be arrested in order to defend these rights, but their agenda remains largely non-violent in nature.

Overall Evaluation: Refugee groups are generally non-violent, but they have been known to protest with physical force in the past. Whether or not the group has the means for cyber-attack is unknown, but increasing escalation in political activity could bring about greater overall activity.

NSW SGE 2015 Evaluation: The level of electronic threat is unknown, but the grassroots structure of the organisation does not point to serious potential for damaging activity. Although the group has been involved in illegal activities in order to free and hide detainees, it remains largely non-physical and non-violent, though its political agenda could see this change in the future with a change in government policies pertaining to asylum seekers and detainees.
Rogue Political Operatives (RPO)

Access: Internal/External
Intention: Advantage, Embarrassment
Boundary: Internal code
Organisation: Individual
Proficiency: Basic
Purpose: Acquire, Damage, Manipulate
Attribution: Clandestine
Affiliations: NA

Date revised: 10 Jan 14

Summary: RPO organisations which might be associated with political party and individual candidate campaigns have a long history of unethical and unlawful activity in the non-cyber world. They are adept at utilising their people and resources to force change in order to achieve their goal. They are typically external but also may place agents within.

Activity: RPO organisation activity has occurred in the cyber domain to attack and promote candidates since the late 1990s, but the only case involving Internet voting was in Estonia in 2011 and 2013. In that case during two party elections, e-votes of elderly members of the ruling party were cast fraudulently by rogue elements within the party. Other examples of cyber activity by RPO include fake websites set up to parody and criticise opponents, defacement of candidate sites and theft of candidates and political party confidential email to discredit them.

In the non-cyber world their activities are well documented and have included distributing false how to vote cards, stuffing ballot boxes, voting for others and various other illegal activities. These RPO may be well funded and use technology on their internal operations. RPO may have, due to their nature, strong ties to local, state and federal government.

Target: RPO are trying to change the outcome of the election by whatever means are available either direct or indirect. Their interest in Internet voting is largely opportunist and seen as another means to achieve their desired end state.

Overall Evaluation: This agent is external but may also have some internal agents due to their political connections. They are pragmatic and wish to promote their candidate/party over others and will use various means to achieve that outcome.

NSW SGE 2015 Evaluation: The election would be a priority target of RPO as they are interested in influencing the outcome of elections and Internet voting is just another opportunity to achieve this. They have shown their capacity to breach the law in furtherance of their aims and have operating in the cyber world. However, they would assess the likely impact of this activity on the outcome before deciding to act and are more likely to utilise non-cyber means which may have a broader effect on an election result.
Syrian Electronic (SEA)

Access: External
Intention: Harm
Boundary: None
Organisation: Formal organisation
Proficiency: Advanced
Purpose: Damage, Denial, Destruction
Attribution: Overt
Affiliations: Syrian Government, Iranian sponsored organisations
Other: Anti-affiliation with Anonymous

Date revised: 10 Jan 14

Summary: The SEA manifests as a virtual army aligned with Syrian President Bashar al-Assad government. Assembled in 2011, the agent uses online vandalism and defacement to push pro-government political agenda, but it has also been linked to DDoS attacks, domain hijacking and general hacking. Recent attacks have shown an increasing level of sophistication, with some theorising the agent is receiving aid from senior government sources and sympathetic high-level hackers. SEA has been touted in underground circles as one of the top 10 most skilled hacking teams in the world, however, others rate the capability as entry level attacks exploiting weak targets or opportunistic hacking with post attack claims (making them look more skilled than they are).

Activity: The SEA has stated being responsible for compromising and defacing hundreds of websites it claims were falsely reporting on the Syrian government. The agent uses Facebook as a popular platform for spamming campaigns, with recent DNS-level redirects from secure servers and DDoS attacks linked to growing sophistication. The agent has also used remote attacks to compromise and hijack web-based communications in order to both gather intelligence on rebel activity and cloak physical pro-Assad attacks. Recently, SEA targeted Qatar in DNS attack in response to Qatar's support of the rebels that redirected many Qatar web sites.

Target: This agent's main targets are political opposition groups and western websites, including news organisations and human rights groups. Among the agent's targets have been the websites of BBC News, The New York Times, The Daily Telegraph, Washington Post, Syrian broadcasters, rights organisations and VOIP applications. They have also target government agencies including the US Military and the French embassy in Damascus. Social media channels are a particularly popular target given their relevance in spreading agenda on a viral level.

In April 2013, hackers claiming to be part of the 'Syrian Electronic Army' claimed responsibility for hacking the Twitter account of Associated Press and sending a false tweet reporting explosions at the White House – which wiped $136 billion off the DOW. In Jan 2014, Syrian Electronic Army also claimed responsibility for hacking Skype in retaliation to the Microsoft's alleged involvement with the NSA links.

Overall Evaluation: Since 2011 the SEA has grown more targeted and ambitious in its attacks and targets, leading to increased surveillance from both the Middle East and West. Although early attacks showed a low level of skill, recent increased level of activity, targeting suggests improved capability, alignment or sponsorship. They are a valid threat when considering the government backing and potential proposed links to Iranian hacking groups.

NSW SGE 2015 Evaluation: The Australian government would be a low priority target for SEA due to little political rhetoric about support by Australia for western lead intervention in the Syrian conflict. The trigger for becoming a higher priority target would be Australian direct involvement in any physical deployment of troops to
Syria or vigorous outward support for the US / western countries to do the same. The election could then become a target to cause major disruption to gain international notoriety for such an attack, but there is a low chance at this point of the timing of iVote being accessible coinciding with escalation of Australian federal government involvement.
System Administrators

Access: Internal  
*Intention:* Advantage, Harm  
*Boundary:* Internal code  
*Organisation:* Individual  
*Proficiency:* Advanced  
*Purpose:* Damage, Destruction, Steal  
*Attribution:* Clandestine  
*Affiliations:* NA

*Date revised:* 10 Jan 14

**Summary:** A system administrator manages and maintains a computer system day to day for an organisation. In this case, they would be responsible for the iVote system and making sure it maintains up time or supporting the infrastructure for the system. They would have privileged access that may be unmonitored or subject to malicious modification.\textsuperscript{vii}

**Activity:** In the past, system administrators have been linked to the leaking of confidential company data in a variety of organisations, including government bodies. Such leaks are typically either politically or financially motivated. In the case of Edward Snowden, who leaked confidential data, the National Security Agency chose to reduce the number of system administrators\textsuperscript{viii}.

In 1999 and early 2000, there were three internal breaches in 18 months at the Australian Defence Intelligence Organisation (DIO). This led to the arrest of multiple individuals, one of which had attempted to sell on 700 classified documents to a foreign embassy. These internal leaks led to a major security review within DIO, including the addition of random bag searches, tighter vetting of staff and assessing their physiological behaviour. More than 50 recommendations to prevent further leaks were prepared by the then Inspector General of Intelligence and Security, with the Australian Security Intelligence Organisation agreeing to undertake an internal and voluntary trial of electronic lie detector equipment.\textsuperscript{cix} In all of these cases, system operators have a privileged level of access to equipment that is vital to conducting the election.

**Target:** Most rogue system administrators are motivated politically and/or financially. Another popular motivation for malicious activity amongst system administrators is disgruntlement. An ex-employee’s knowledge of system protocol and credentials may allow them access to a network long after their employment has been terminated and poses a substantial security risk.

**Overall Evaluation:** Research suggests that up to 40% of systems administrators abuse their position by illegally monitoring personal employee files and emails. Such information could be used by an administrator to manipulate or leak private information about the election, with the system administrator’s position allowing them to possibly delete logs to cover their tracks effectively.\textsuperscript{cx}

**NSW SGE 2015 Evaluation:** iVote system administrators may have access to potentially manipulate and leak confidential information or affect the election. The administrator’s role also allows them better access for covert activity and erasure of incriminating logs and files.
### Threat Actor Attribution Matrix

This matrix provides a graphical representation of the threats actors and their attributes for NSW SGE 2015. (Definitions can be found in Appendix B).

The outcome from this analysis determines that the threat actor attributes, in order of magnitude, will manifest themselves in the form of an attack that is:

- Driving an outcome to the advantage of the threat actor.
- Actions will likely be of an illegal nature to Australian / International law and instead driven by their own internal code of conduct that they believe supersedes such law.
- Most actions will have the support and resources of an individual; however formal organisational efforts are represented strongly.
- Attacks will be equally spread between basic to advanced in nature.
- The main objective will be to steal data (leave the data intact) from the iVote application, system or process. However, objectives strongly represented are also to damage or manipulate such data.
- The nature of the attack is likely to be clandestine or overt in nature. To either support the theft of information, its manipulation, or cause reputation damage by disruption.

![Threat Actor Attribution Matrix](image-url)
Attack Trees

These attack trees are conceptual diagrams representing how an asset, or target, might be attacked. Attack tree structure allows a systematic approach to threat analysis by a formal, methodical way of describing the security of systems, based on varying attacks. It covers up to the point of execution of the attack with post-attack actions not covered as it is irrelevant to the definition of an attack tree and this analysis to focus defensive measures.

The attacks trees outlined below are focused on the types of attacks against an electronic voting system. It does not represent the exact environmental architecture for NSW SGE 2015, which is part of Phase 1B of the engagement.

There are three types of nodes:

- **AND** – All dependants must be achieved in order for this type of attack to occur.
- **OR** – These are alternatives. In some cases the attacker could use multiple methods but they only need to satisfy one node for the attack to occur.
- **EVENT** – An attack occurs based on the path taken to reach this node.

The full table of attack trees can be found in the full report.

Figure 2 - Attack Tree - Internet Voting - Overview
**Tabletop exercise**

The tabletop exercise is a wargame designed to take each of the attack trees and exhaust them through a joint workshop. Each attack tree is stepped through with the key NSWEC staff reacting to a threat actor’s attacks to test their defences, which in turn can spark a reaction by the threat actor and this continues until an attack tree is stopped due to defensive measures, not possible due to the environment or an exposure is identified. The session is recorded in full to capture all points and decisions made and can be found in Appendix D.

The exercise was held with four CSC security consultants fulfilling the roles of co-coordinator, recorder, threat actor and attack specialist. NSWEC was represented by the CIO and two others.

Details of the tabletop exercise can be found in the full report.
Threat Courses of Action

The table top exercise attack tree exposures are compared to the known threat actor capabilities and probable intentions to provide an order of magnitude to the threats faced for the SGE 2015. The focus is on this analysis is on the course of actions and associated attacks where there are potential exposures in the system.

Combined Threat Capability and Exposures

The following matrix combines the early threat actor capability with the exposures identified during the workshop. It allows for the analysis between the exposures to address and the threat actor known capabilities. The Attacks highlighted in grey in the table are the courses of actions assessed:

The following courses of action and associated potential attack taxonomies are related to only the threat actors with medium and high capability levels. Only the phishing attacks taxonomy for low capability has been detailed, as there are no threat actors with assessed medium to high capability.

Most likely courses of action

The most likely courses of actions and associated attack trees are based on the analysis of the threat actors, the potential exposures and historical attacks. In no partial order they are:

1. **Denial of Service (DoS)** – Many threat actors have the capability to conduct a DoS and DDoS attack, whether as part of an inherent capability or easily obtainable in the black market for cyber attacks. The most likely course of action for DoS would take the form of an attack during the election to cause disruption, denial and/or embarrassment to the NSW SGE 2015 and / or the use of electronic voting.

   The most likely form of the attack will be against the iVote application from the Internet by directing many concurrent connections against the application or attempting to consume all server resources, such that the application is slow and cannot process transactions in a timely manner.

   Further details can be found in the full report.

2. **Registration Database attack (Voting server attack)** – Some threat actors have the opportunity to compromise the registration database. The most likely course of action would take the form of an attack during the election to affect the election outcome and ultimately cause embarrassment to the NSW SGE 2015 and / or the use of electronic voting.

   Given a precedent with respect to a successful historical attack on the registration database, the most likely form of any future attack would be against the registration database from outsiders by
compromising the web-based application through the discovery of recent vulnerabilities and the potential to exploit these. Attacks from insiders are unlikely given the established process by NSWEC to incorporate dual control for administration access.

Further details can be found in the full report.

3. **Phishing Attacks** – Some threat actors have the opportunity to orchestrate a phishing attack against registered voters. The most likely course of action would take the form of an attack prior to and during the election to affect the election outcome and ultimately cause embarrassment to the NSW SGE 2015 and/or the use of electronic voting. The most likely form of any future attack will be to target registered voters and lure or convince them to vote for a certain candidate or party in order to achieve their motive.

iVote contractors for the SGE 2015 can also be targeted by phishing attacks (such as software developers, auditors, security providers, etc) as a precursor to gain logical access or other malicious acts.

Even though NSWEC staff may be targeted attacks from insiders are unlikely given the established process by NSWEC to incorporate dual control for administration access.

Further details can be found in the full report.

**Most Dangerous courses of action**

Given the consequence of a particular course of action the following possible, but not probable attack that could result is:

4. **Malicious Application** – As there will be a lock down period where all access to systems and applications will be removed, apart from a few privileged users, before ‘Live’, the only time to which a malicious application could be implemented on either an application or hardware is prior to the lock down period.

There are a number of Threat Actors who have shown the capability to implement a malicious application in an environment to which they wish to manipulate or impact. In this case it could mean altering the outcome or disrupting the NSW SGE 2015. This would be one of the most dangerous course of action due to being able to operate undetected.

Further details can be found in the full report.

5. **Modification of audit log data** – Audit logs are used to verify all activities conducted on both systems and applications. Modification of the logs would be the most dangerous course of action because if the logs were altered in any way the reliability of the systems and applications logs would be lost. This includes directly altering the database which stores the logs or altering the systems generation of logs, altering NTP or altering the applications log configurations.

Two Threat Actors have shown the capability to modify audit log data. In this case it could mean loss of integrity of voting process for the NSW SGE 2015, which would be one the most dangerous course of action.

Further details can be found in the full report.
Trigger points

Trigger points are events that occur that could be the precursor to a particular course of action and hence attack being carried out by a threat actor. Trigger points represent where a decision must be made by a threat actor that will result in inaction, action or an alternative action.

A number of trigger points have been identified and are included in the full report.

Named Areas of Interest

Named areas of interest are zones where trigger points are likely to surface and be exposed. These zones form a critical part of a proactive defensive strategy as they will provide potential early warning of an impending attack by a threat actor. Named areas of interest will then feed into the overall intelligence requirements and collection planning as per the table in the next section.

A number of Named Areas of Interest have been identified and are included in the full report.

Intelligence Requirements / Collection Plan

The following is the foundation of the Intelligence Collection plan for the SGE 2015. This provides focused areas of further research and areas to monitor validate assumptions, capture threat actor actions or assist with the employing effective defensive measures. It is recommended that the a plan is followed and tracked to assist with the collection of information related to threat actors and potential attacks, it may provide a proactive defensive measure to the SGE 2015.

The Intelligence collection plan is included in the full report.
**Recommendations**

The following recommendations are based on the analysis of the environment, tabletop exercises, exposures and correlation with the threat actors that resulted in the courses of actions. This is based on the information given and provided by NSWEC and subject to change if any of the assumptions are validated or eliminated.

**Technical security controls**

- Manipulate audit logs
  - Implement an independent Network Time Protocol (NTP) – Implement an independent NTP that is fully controlled by NSWEC and synchronises its date and time service via GPS with a satellite. This would become an independent authoritative time service (stratum level 1) only accessible by NSWEC.
  - Monitor NTP – Monitor and assess all changes made to the NTP service to validate that they have been appropriately authorised. Changes to NTP may be used by an attacker to hide further malicious activity by modification of date time stamps of logs.
  - Implement Secure NTP - Identity Schemes are methods to prove the identity of a remote system, helping to prevent man-in-the-middle attacks. In NTP Security Algorithms and NTP Security Model the following identity schemes are mentioned:
    - Private Certificate (PC)
    - Trusted Certificate (TC)
    - Schnorr Identity Scheme (IFF)
    - Guillou-Quisquater Identity Scheme (GQ)
    - Mu-Varadharajan Identity Scheme (MV)
  
  The PC scheme is much like private keys, requiring a secret channel to distribute keys. The TC scheme uses a trusted authority (TA) and certificate chains. The IFF scheme uses DSA principles. The GQ scheme is based on RSA principles. The MV scheme is based on DSA principles also, but does not require trusted clients.

  All schemes use relatively small keys (few bits), so that those keys must be refreshed regularly. Even though certificates are valid for one year after creation, the keys should be re-created on a shorter interval. Using the NTP timestamp as the certificates’ serial number ensures uniqueness. Thus signatures are only generated when the host’s time is considered synchronized.

  - Monitor logging systems and logs generated – Monitor and assess all logging systems by audit log trails and other information to validate that they have been appropriately authorised. This would ensure the integrity of the centralised logging facility and SIEM correlation systems. The logging solution should be able to handle standard and peak message rates and demonstrate predictable and manageable behaviour under high volume events and situations in which system resources such as network, CPU, memory or storage are exhausted.

  - Test source log generation. The iVote system logging generation should be tested to ensure logs are generated as expected. This would address any malicious code that is suppressing or changing logs to hide further malicious activity. This functionality testing should include at a minimum the following performance and behaviour attributes:
    - Real world and synthetic message generation for both expected and burst rates.
    - Date and time of event attributes (malware that is active during a specific window of time).
    - Storage and message capacity behaviour.

- Compromise application
Independent security review of software code – An independent third party (neither NSWEC nor the 3rd-party software developer) reviews and assesses the iVote application for vulnerabilities, such as logic errors, manipulation of data, provision of erroneous audit trail information or the implementation of backdoor access. This is typically facilitated through a software code review tool and/or manual code review.

Penetration Test – The penetration test undertaken should review the accessibility of the iVote application from an external presence for the most common network and application-based attacks. The scope for the penetration testing should preferably include;

- Web application testing.
- Internal and external network testing.
- Technology compliance assessment.
- Social engineering attacks against NSWEC staff and contractors.
- A test of the physical premises hosting NSWEC iVote information systems and assets.

Monitor iVote Web Server – Monitor the web server statistics for any unusual activity that indicates reconnaissance activities are being undertaken. This is typically an indication of an external malicious actor attempting to exploit vulnerabilities. This solution should be complimented by a centralised audit logging and assurance service to increase availability and fidelity of data or analysis.

Network attacks

- DDoS protection – It is recommended that NSWEC engage a Tier-1 “Big-Pipe” solution to DDoS mitigation. This has a number of significant advantages to NSWEC. This form of upstream protection allows NSWEC to effectively mitigate DDoS attacks at their source rather than their destination. Several methods other methods of DDoS protection were considered including public cloud infrastructure and Content Distribution Networks however they were not considered optimal to meet NSWEC’s specific requirements. In this case, it is undesirable from a security perspective to relinquish control of the applications SSL certificated to a public cloud or content delivery network.

System configuration and settings – Server systems should be configured according to vendor and/or industry guidelines to enable appropriate system settings that assist the server to self-defend against attacks targeting the consumption of server resources. The effectiveness of the final configuration should be comprehensively assessed and validated during planned penetration testing activities.

Firewall settings – Firewall global settings should be configured according to vendor and/or industry guidelines to limit the number of concurrent connections to minimise the impact of DDoS attacks. Industry best practice should be applied and reviewed as part of a firewall audit.

Web Application Firewall (WAF) – NSWEC should customise their WAF rules to the iVote application, many attacks can be identified and blocked that would evade standard protection mechanisms such as Layer2/3 firewalls and even application aware IPS. The effort to perform this customisation can be significant and needs to be maintained as the application is modified. Due to this additional requirement, it is recommended that a service provider or consultancy group familiar with this customisation be engaged to configure, tune and test the end solution.

When considering selecting a WAF for NSWEC they should consider that they are typically offered in two mature and one developing format and should be considered based on their respective attributes versus NSWEC’s requirements and architecture.

- Server / Module Base: Service modules for common web servers including IIS and Apache include examples such as ModSecurity. They provide the ability to perform request filtering and other security within the web server itself. A comparative penetration testing analysis report was published by Zero Science Lab (Feb/2013), showing that ModSecurity is more effective than offerings such as CloudFlare and
Incapsula, but it demonstrated a greater rate of false positives than its competition. Server modules, while effective at resolving and protecting against application errors and vulnerability, do suffer from a performance impact on the host server aggravating the effect of denial of service based attacks.

- Appliance Based: Dedicated hardware that can effectively address and scale against local web services. Vendors such as Imperva, currently considered the WAF leader, offer appliances dedicated to web application functionality and protection. They however lack the ability to perform Tier-1 DDoS protection and should generally be considered as a complimentary / dependant mechanism for web applications at risk of large scale network based DDoS attacks.

- Cloud Based (emerging): Companies like Akamai Technologies offer cloud-based WAF that incorporates advanced features such as rate control and custom rules enabling it to address both layer 7 and DDoS attacks. They do however require the site to relinquish control of their SSL certificates to the host.

- Internet service providers – The Internet service providers that NSWEC utilises should be able to demonstrate the ability to dynamically increase bandwidth using a golden screwdriver approach during SGE 2015 to provide more bandwidth as required.

Non-Technical security controls

- Compromise application
  - Background checks – Ensure that appropriate screening of employees and contractors employed by the successful 3rd-party software developer is undertaken and written into any contractual agreement between NSWEC and the software developer.
  - Roles and responsibilities – Ensure that a roles and responsibilities matrix exists for all stages of the software development process.

- Network attacks
  - Domain Name Service (DNS) – The solution should monitor and assess all changes made to the DNS service to validate that they have been appropriately authorised.

- Voter server attack
  - Registration database – Implement a process to monitor and respond to unauthorised access of the voter registration database.

- Process attack
  - Security awareness and training for iVote users – Develop and deliver training for Internet voters on the types of attacks used against web-based voters, such as those delivered via SMS or email.
  - Security awareness and training for call centre staff – Develop and deliver targeted training for call centre staff on managing cyber attacks and anomalies that may manifest due to the use of web-based voting. This can include monitoring the influx of unusual email or phone calls (most likely phishing attacks).
  - Security awareness training for NSWEC staff – Develop and deliver targeted training for staff on social engineering and physical presence attacks that could be a precursor for a technical attack.
  - Security awareness training for 3rd party Contractors – Ensure that contractors employ an effective security awareness training package focused on iVote and the potential threats such as subversion, phishing, malware, physical reconnaissance, etc.

- Physical attack
  - Surveillance of premises – the monitoring of the data centre and servers rooms was covered adequately during the workshop. However, further direct workplace monitoring of NSWEC and associated contractors may be warranted to provide further defence against social engineering
attacks.

It is recommended surveillance would complement the staff / contractor security awareness training and surveillance could be simply heightened awareness of visitors, third parties and the public where staff are encouraged and have a mechanism to report strange activity, approaches or questioning relating to NSWEC use of electronic voting.

Other

The following are other recommendations based on the analysis that are not strictly security controls:

- **Updating of threat actors** – Initially quarterly with increasing frequency leading up to the SGE 2015 which will provide visibility for any changes in motives, modus operandi, capability, intentions or affiliation.

- **Media Coverage** – Leading up to the SGE 2015 the NSWEC should monitor the media for any events that might act as a catalyst or be a potential pre-cursor to an attack. The main areas that NSWEC should be looking at are:
  - International affairs where Australia might be the target for controversial policy or actions – this may result in the SGE 2015 becoming a target of opportunity.
  - Increased national or international general media coverage of the SGE 2015 and its use of electronic voting.
  - Any actions or rhetoric by known threat actors that could result in the attacks.

- **Monitor key contractor employment additions** – Through the contractor appointed Account Manager or Human Resources team be made aware of any new employees to the organisation that are undertaking a key role in the development of iVote. Assessment or background checks of that employee could be made to verify no linkage to any threat actor.

- **New controversial / emotive legislation** – NSWEC should make themselves aware of any new (or changes to) legislation or policy that would be seen as controversial to either the public or threat actors. NSWEC should be looking for heightened tensions around the new legislation / policy and focus further collection efforts on associated action groups that may targeted the SGE 2015.

- **NSW police, AFP and Australian Intelligence community liaison** – would assist the NSWEC with any known criminal groups, criminal elements or potential individual suspects that may have the capability and the desire to target iVote for the SGE 2015.

- **Monitoring of the workplace and employees for unusual behaviour** – NSWEC should assess and know the critical direct and contractor staff working on the iVote project and put in place additional Human Resource supported monitoring through management to provide assurance that any unusual or suspect behaviour is captured that could result in rogue actions.

- **Monitoring of key web pages** – closer to the SGE 2015 NSWEC should monitor web pages that might provide a precursor to a threat actor’s action. This would include at a minimum monitoring of blogs, websites, and forums associated with:
  - Anarchist groups
  - Protester / Action groups
  - Known Threat Actors sites
  - “Black market” sites
Appendix A – Definitions and Acronyms

Important to accurately define for comparison and standardisation:

- **Course of Action**: is a theoretical action that a threat actor can take, that is base off capability and the known possible attack trees.

- **Internal Threat Actors**: this includes NSWEC officials (including on the day election staff), government officials (state and Federal) and third parties employed by government.

- **External Threat Actors**: by definition all others not covered by the Internal Threat Actors, but in particular includes the political parties.

- **iVote**: is the system that NSWEC is using for Electronic Voting (eVoting) which is a Remote Electronic Voting (REV) system. iVote allows electors to cast their vote using telephones or computers with browsers and internet access.

- **Named Area of Interest**: are areas where key events, or trigger points may be observed and form part of the overall intelligence collection plan.

- **NSWEC**: New South Wales Electoral Commission.

- **Remote Mode**: this is the act of an iVote user conducting their vote on a web enabled computer device.

- **SGE 2015**: NSW State General Election 2015.

- **Terrorism**: No international term defined. Using the Commonwealth legislation definition “The Criminal Code Act 1995 states that a terrorist act means an action or threat of action where the action causes certain defined forms of harm or interference and the action is done or the threat is made with the intention of advancing a political, religious or ideological cause”.

- **Threat Actor**: This is the person of organisation carrying out the action; in this case the action outlined in the attack tree. The threat actor will have a number of influencers or sponsors with a vested interest who will have overt or covert characteristics, but they will not be included as a threat actor.

- **Trigger Point**: A trigger point is the catalyst to a course of action by a threat actor and can also be a represent a point where a decision has to be made that may form an alternative course of action.
Appendix B – Threat Actor Attribute Definitions

The threat actor attribute definitions help provide a summary view of the various characteristics within the scope of the identified threat actors to the NSW SGE 2015 in respect to iVote. It allows for a focused approach to the potential magnitude of combined effects that the various threat actors can bring to the event, but does not provide an assessment of likelihood, individual damage assessment or consequence - this is formed as part of the risk assessment process when overlayed with the technical environment.

1. Access
This provides the level of access that the threat actor has to the system:
- **Internal**: Agent has internal access.
- **External**: Agent has only external access.

2. Organisation
This assists with defining the level for resources and support the threat actor has at its disposal to conduct any given activity. The highest one is chosen:
- **Individual**: The threat actor will only have themselves as an available resource and they generally act independently. (ie. The opportunistic hackers that conduct malicious activity for the fame of it).
- **Informal Organisation**: Network of personal and social relationships (alliances, cliques, friendships) that arise as people associate with other people. They have a common theme or goal that binds them and generally an informal leadership based on technical prowess. (ie. Anonymous).
- **Formal Organisation**: People operate under a fixed set of established rules and leadership that provides governance through formal or informal procedures and operations. (ie. organised crime).
- **Government**: Larger and better resourced than an organisation and can operate within their own legal jurisdiction that may counter international law. Funding and resource limits are far greater than the other groups, but they operate under a very bureaucratic framework that can hinder their operational flexibility and reaction.

3. Proficiency
The special training or expertise an agent typically possesses. Options are:
- **None**: The threat actor is of average intelligence but has no formal training or exposure to information technology that would allow them to carry out any attack worthy of mentioning.
- **Basic**: The threat actor can carry out rudimentary malicious acts that are available for purchase in preconfigured code. Such attacks are normally limited to acts of disruption or destruction, but have no expertise or training in the specific methods necessary for a targeted attack. Example: Untrained Employee.
- **Intermediate**: The threat actor has the ability to create general attacks or modify existing malicious attacks to provide a more focused approach. Normally such a threat actor is limited to one or a few domains of expertise and will heavily rely on these to conduct their activities. Example: General information technology employee.
- **Advanced**: Expert in the technology stack, manipulation of code to take advantage of all layers and exposure to multiple attack methods. They are capable of create new malicious code or methods to take advantage of known or unknown vulnerabilities. They also may show proficiency in social engineering. Example: Anonymous

4. Boundary
This provides the limit to which the threat actor is bound to operate within. This maybe associated from their organisation or other influences.
- **International Law**: The threat actor would adhere to international law and operate within its bounds.
• **National Law** – The threat actor will operate within their nation state legal boundaries or government wishes, which may not align or breach international law.

• **Internal Code** – The threat actor does not care for legal boundaries, but is instead governed by an internal or strong personal code. These may or may not conflict with international or national law.

• **Religious** – The threat actor is strongly bound to their interpretation of their chosen religious beliefs and that of their religious leaders. These may or may not conflict with international or national law.

• **None** – The threat actor has no bounds and will act without fear of any legal, code or religious boundaries.

5. **Intention**
   This details the threat actors desired endstate for the attack against its target.

   • **Advantage** – The threat actor seeks to modify, steal or add to a target's asset or data that would provide them or their cause an advantage.

   • **Harm** – The threat actor wants to damage its target so that its assets or data are modified to the point that recovery or reconstruction is required. This goes beyond embarrassment which should be technically recoverable.

   • **Embarrassment** – The threat actor wants to cause brand or reputation damage to its target that may not have much of a real asset or data affect, but rather loss of faith or distrust with the targets’ customer base.

   • **Loss** – The threat actor seeks to make its target loose assets or data that cannot be recovered.
     (ie. Destruction of nuclear power plant plans)

6. **Purpose**
   The purpose are the actions available to the threat actor that aligns with their modus operandi in order to achieve their intention:

   • **Acquire**: This action by the threat actor is focused toward the acquisition of content or ownership of an asset (virtual or physical) without further modification or removing it from the target's use. (ie. Copying of intellectual property to sell to others to breach copyright).

   • **Damage**: Causing damage to an asset through modification that degrades its worth or has limited function (ie. Modification of a website’s functionality to that does not allow users to perform e-commerce transactions).

   • **Denial**: This action seeks to deny access to content or an asset to one or many users. (ie. A DDOS attack on a web server so users browsing cannot see the website).

   • **Destruction**: Destruction of the targeted content or asset to render it worthless to all, including the threat actor. (ie. Deletion of content on a fileserver).

   • **Manipulate**: Modification of data, asset or content for the purposes of achieving a stated aim or result (ie. encryption of documents for ransom purposes).

   • **Steal**: This is the act of simultaneously acquiring the asset by the threat actor and removing the asset so it cannot be used by the target. (ie. Removing credit card details from an e-commerce site).

   • **Indifferent**: The threat actor is more opportunistic and will seek to do whatever they can to the target or the target is an attack of opportunity. (ie. A low technical hacktivist emotionally reacts to a target’s public announcement and conducts a variety of scans to find a weakness to discredit the target).

7. **Attribution**
   Attribution outlines the level of exposure and secrecy the threat actor aims to have either their attack or identify known. Only one attribute can be chosen and it must be the most visible level for that threat actor if they operate at various levels of secrecy.
• **Overt**: The threat actor conducts the activity with the intention of making the attack and their identity known before, during or after the attack. (eg. Anonymous’ attack against web sites to bring them down).

• **Covert**: The threat actor conducts the activity with the intention of maintaining secrecy of their identity, but making the attack visible (eg. Stutzex attack trying to achieve secrecy of their identity).

• **Clandestine**: The threat actor conducts the activity with the intention to maintain secrecy of both the actor and their identity. (eg. An attack to steal intellectual property from a foreign sponsored organisation).

• **Not Applicable**: The threat actor does not consider the implications of secrecy of their identity or that of the attack or does place any importance on secrecy. (eg. A hacktivist who reacts emotionally to a target and looks for a quick attack of opportunity).
Cybersecurity
Level 2/Tower B
26 Talavera Road
Macquarie Park, NSW 2113
Sydney, Australia
+61(0)2.9034.3000

World CSC Headquarters
The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Asia
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

Australia
Level 6/Tower B
26 Talavera Road
Macquarie Park, NSW 2113
Sydney, Australia
+61(0)2.9034.3000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

About CSC
The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients and improve operations. CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC leads with an informed point of view while still offering client choice. For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs. The company trades on the New York Stock Exchange under the symbol “CSC.”