Editorial Panel

Editor-in-Chief
- Ts. Dr. Zahri Yunos, CyberSecurity Malaysia (Malaysia)
- Professor Ts. Dr. Rabiah Ahmad, Universiti Teknikal Malaysia Melaka (Malaysia)

Associate Editors-in-Chief
- Mohd Shamir Hashim, CyberSecurity Malaysia (Malaysia)
- Dr. Shekh Faisal Abdul Latip, Universiti Teknikal Malaysia Melaka (Malaysia)

Editorial Board
- Dato’ Ts. Dr. Haji Amirudin Abdul Wahab, CyberSecurity Malaysia (Malaysia)
- Abdul Hakeem Ajijola, Consultancy Support Services Ltd (Nigeria)
- Ts. Dr. Aswami Fadillah Mohd Arifin, CyberSecurity Malaysia (Malaysia)
- Associate Professor Dr. Azni Haslizan Ab Halim, Universiti Sains Islam Malaysia (Malaysia)
- Engr. Badar Al-Salehi, Oman National CERT (Oman)
- Hatim Mohamad Tahir, OIC-CERT Professional Member (Malaysia)
- Ts. Dr. Mohd Fairuz Iskandar Othman, Universiti Teknikal Malaysia Melaka (Malaysia)
- Dr. Muhammad Reza Za’ba, University of Malaya (Malaysia)
- Dr. Muhammad Salman Saefuddin, Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center (Indonesia)
- Associate Professor Ts. Dr. Noor Azurati Ahmad@Salleh, Universiti Teknologi Malaysia (Malaysia)
- Shamsul Bahri Kamis, Brunei Computer Emergency Response Team (Brunei)
- Ts. Dr. S.M. Warusia Mohamed S.M.M Yassin, Universiti Teknikal Malaysia Melaka (Malaysia)
- Ts. Dr. Solahuddin Shamsuddin, CyberSecurity Malaysia (Malaysia)
- Professor Dr. Zulkalnain Mohd Yusoff, Universiti Teknikal Malaysia Melaka (Malaysia)

Technical Editorial Committee
- Ahmad Nasir Udin Mohd Din, CyberSecurity Malaysia (Malaysia)
- Ts. Dr. Aslinda Hassan, Universiti Teknikal Malaysia Melaka (Malaysia)
- Dr. Nur Fadzilah Othman, Universiti Teknikal Malaysia Melaka (Malaysia)
- Noraini Abdul Rahman, CyberSecurity Malaysia (Malaysia)
- Dr. Raihana Syahirah Abdulllah, Universiti Teknikal Malaysia Melaka (Malaysia)
- Dr. Sofia Najwa Ramli, Universiti Tun Hussein Onn Malaysia (Malaysia)
- Ts. Dr. Zaki Mas’ud, Universiti Teknikal Malaysia Melaka (Malaysia)
Content

Practical Guideline for Digital Forensics Laboratory Accreditation – A Case Study
Sarah Taylor, Akmal Suriani Mohamed Rakof, and Mohd Zabri Adil Talib

The Integration of Cyber Warfare and Information Warfare
Noor Azwa Azreen Binti Dato’ Abd. Aziz, Engku Azlan Bin Engku Habib, and Madihah Mohd Saudi

Cyberbullying via Social Media: Case Studies in Malaysia
Azriq Ariffin, Nurul Mohd, and Thurgeaswary Rokanatnam

Establishment of a Method to Measure the Awareness of OIC-CERT Members
Tural Mammadov, Noraini Abdul Rahman and Mohamad Farhan Mohd Rahimi

Development of Examination Framework for Cyber Security Professional Competency Certification
Siti Rahayu Selamat, Lee Hwee Hsiung and Robiah Yusoff

Overview of Prioritization Model for National Critical Sectors Protection
Ariani and Muhammad Salman

Achieving 5G Security through Open Standards
A. Cheang, X. Gong, and M. Yang

New Vulnerabilities upon Grain v0 Boolean Function through Fault Injection Analysis
Wan Zariman Omar@Othman, Muhammad Rezal Kamel Ariffin, Suhairi Mohd. Jawi, and Zahari Mahad
Practical Guideline for Digital Forensics Laboratory Accreditation – A Case Study

Sarah Taylor, AkmalSuriani Mohamed Rakof, and Mohd Zabri Adil Talib
Digital Forensics Department, CyberSecurity Malaysia, Cyberjaya, Malaysia
sarah@cybersecurity.my

ARTICLE INFO

Article History
Received 04 Feb 2020
Received in revised form 07 Dec 2020
Accepted 08 Mar 2021

Keywords:
Digital forensics;
Digital forensics accreditation;
Forensic lab management

ABSTRACT

Digital forensics is a branch of forensic science that is used to assist investigation of cybercrime cases. Digital evidence, such as from mobile devices and computers, are analysed and the data are interpreted to assist the court of law in understanding what has taken place. In order to provide an assurance to the stakeholder on the accuracy of the forensic result, ISO/IEC 17025 has been used by forensic accreditation bodies to accredit laboratories. This paper, presents the case study in getting a digital forensics laboratory accreditation, the methodology, and the lesson learnt. This paper is hoped to provide guidance to those who would like to pursue accreditation for their Digital Forensics Laboratories (DFL).

1. INTRODUCTION

Digital forensics is defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence. These evidences are derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations [1].

Digital forensics is used in investigation of crime cases. The digital evidence is analysed and the data are interpreted to assist the court of law in understanding what has taken place.

In order to provide an assurance to the stakeholders on the accuracy of the forensic results, a standard is applied to the work produced by a laboratory [2][3][4]. A notable standard for digital forensics laboratory (DFL) is the ISO/IEC 17025 [5].

This paper aims at presenting a case
study in obtaining accreditation for DFL. The work provides the following contributions:

- Methodology on getting accreditation.
- Lessons learnt in the journey of obtaining accreditation in order to increase the success rate.

II. BACKGROUND

A. Overview of the ISO/IEC 17025

The ISO/IEC 17025 General Requirement for the Competence of Testing and Calibration Laboratories specifies the requirements for a laboratory to perform its works [6]. This standard is applicable to all testing and calibration laboratories regardless of the number of personnel or the extent of the scope of testing and/or calibration activities.

Since this standard is meant for any laboratories, generally it is not sufficient for a DFL. Hence accreditation bodies, such as the ANSI National Accreditation Board (ANAB) from USA [7] and the Department of Standards Malaysia [8], produced supplemental requirements specifically for DFLs to fill in the gaps. This document adds critical requirement such as chain of custody and the requirement for the proficiency of analysts.

This ISO outlines 5 major requirements for DFL as follows:

i) General Requirement
ii) Structural Requirement
iii) Resource Requirement
iv) Process Requirement
v) Management System Requirement

![Fig. 1: Digital Forensics Laboratory (DFL) accreditation based on ISO/IEC 17025:2017 standard and accrediting body’s supplemental requirement](image)

The General Requirement addresses confidentiality and impartiality statements. The Structural Requirement, on the other hand, addresses the legality of the laboratory and overall responsibility of the lab and its organization. The Resource Requirement specifies the requirement for personnel, laboratory environment, equipment, and contractors. Meanwhile, the Process Requirement touches on request from stakeholder, methods, exhibits, reporting of results, complaints, nonconforming works, and control of data. The last requirement, the Management System, addresses risk management, corrective actions, internal audits, and management review.

B. Overview of accreditation

The ISO standard can be applied in DFL through self-regulation or accreditation [9]. Self-regulation depends on self-assessment and
attestation. Accreditation refers to the formal recognition by an independent body, known as the Accreditation Body, using technical experts that a DFL operates according to ISO/IEC 17025. ANAB [10] and the American Association for Laboratory Accreditation (A2LA) [11] from US, the National Association of Testing Authorities (NATA) [12] from Australia, and the United Kingdom Accreditation Service (UKAS) [13] from United Kingdom are examples of accreditation bodies.

In US, a consensus regarding accreditation has been reached through the summary of 13 recommendations made in the 2009 National Research Council report entitled “Strengthening Forensic Science in the United States: A Path Forward”. Among the recommendations are to mandate accreditation for all laboratories and facilities (public or private) and mandate individual certification of forensic science professionals [14], depicting the importance of obtaining an accreditation.

According to J. Kolowski [15], with accreditation, DFL is able to put a quality system in place and operational; demonstrating to stakeholders that the work is in good quality and provides a sense of assurance that work is done right.

Considering the erroneous convictions associate with the report from forensic scientist [16], which have caused lasting effects on people’s lives, one might consider implementing a quality assurance in place to prevent such case from happening. The ISO 17025 accreditation, in general, does provide a minimal quality assurance for DFL.

C. Overview of Case Study

The Digital Forensics Department of CyberSecurity Malaysia has successfully obtained accreditation from the US accreditation body in 2011. The department has also successfully maintained its accreditation status until now.

Since the issuance of accreditation, it was observed that analysts were able to answer questions in court more confidently and less mistakes were made particularly human error such as grammatical erroneous in reports due to improper quality assurance in place.

In 2016, CyberSecurity Malaysia received a request from a middle east country to provide consultancy services in obtaining ISO/IEC 17025 accreditation. Not only have the agency successfully obtained the accreditation for the Client, but it has also successfully obtained it in just 14 months. The process of obtaining the accreditation will be explained in section III.

III. METHODOLOGY

The methodology that was used for obtaining the accreditation involves 8 major phases. Fig 2 shows the phases in a nutshell.

The first phase was conducting user requirement study. In this phase,
gaps between current practices and ISO requirements were identified and presented in a report. This process took 2 weeks.

The next phase was to develop the forensic process in writing. The documents that need to be developed were quality manuals, policies, procedures, technical procedures, and forms. Input from analysts were heavily sought in order to create an adaptable process flow. Creativity in developing a short process flow, and covers all essential forensic elements was crucial. The whole process took 8 weeks to complete.

With the process there and the analysts have been trained with the process, next was to implement the process. During this period, the Client must implement the forensic processes by themselves. Records must be created in order for the accrediting body to assess the implementation.

Phase 6 was the Client undergoing an internal audit. Three (3) auditors have been assigned to audit the Client’s laboratory to ensure compliance with the ISO standard. The audit took 1 week, and the auditor took another week to produce the audit report. At the end of 2 weeks, the report was submitted to the Client.

Next, during Phase 7, the Client conducted the remedial phase based on the findings observed during the internal audit. In this phase, the laboratory must resolve issues raised by the auditors. Our Client thankfully did not encounter major issues, hence remedial works took a short period of time, which was only 2 weeks.

At the end of the process, an application for accreditation was submitted to the accrediting body. In order to assess DFL readiness, the lab needs to submit the written forensic process and internal audit report. Once they are satisfied with the developed documents, two (2) external auditors were sent by the accrediting body to observe implementation onsite. No major issues were observed by the auditors, and hence accreditation was
issued to our Client. This whole process took 2 months to settle. In overall, it took our Client 14 months to obtain accreditation from the first engagement with CyberSecurity Malaysia.

IV. DISCUSSION

Based on the observation of the whole accreditation process, it was found that it was doable to get accreditation in a short period of time, provided the lab is coached by experience personnel. The observations on other labs, particularly CyberSecurity Malaysia, on average it took between 3 to 5 years before a lab is awarded an accreditation. With the developed methodology, CyberSecurity Malaysia was able to shorten the duration to get the Client’s lab accredited.

Second observation is that any labs that would like to pursue accreditation must undergo ISO 17025 training, including the senior management. This is important because without a good basic understanding of the ISO requirements, the implementation becomes difficult. For the analyst, when implementation was first introduced, they were having a hard time in understanding the extra work that they need to do. With basic ISO training, it will assist the management in explaining its importance and for analyst to understand the relevancy of the works.

Third observation was that in order for the internal and external auditors to audit the lab work, the lab must have real cases. These cases must be documented so that the auditors and assessors could evaluate the works.

The fourth observation was strong commitment and cooperation from the Client in order to keep up with the planned schedule. In this case, the Client had provided full commitment towards the plan and hence the success in obtaining accreditation in short period of time.

V. CONCLUSION

This paper presented a practical guide in obtaining ISO 17025 digital forensic lab accreditation. The methodology as well as the lessons learnt throughout the whole journey were listed. Future work would be to measure the effectiveness of having accreditation in a DFL.

VI. REFERENCES


The Integration of Cyber Warfare and Information Warfare

Noor Azwa Azreen Binti Dato’ Abd. Aziz¹, Engku Azlan Bin Engku Habib², and Madiah Mohd Saudi³

¹,²CyberSecurity Malaysia, Selangor Darul Ehsan, Malaysia
³CyberSecurity & Systems (CSS) Unit, Universiti Sains Islam Malaysia (USIM)

¹azreen@cybersecurity.my, ²azlan@cybersecurity.my, ³madihah@usim.edu.my

ARTICLE INFO

Article History
Received 20 Mar 2020
Received in revised form 25 Jan 2021
Accepted 08 Mar 2021

Keywords:
Cyber Warfare,
Information Warfare,
Cybersecurity,
Warfare,
Cyberspace.

ABSTRACT

Throughout the years, the appearance of cyber warfare and information warfare have changed and enhanced the methods, techniques, as well as the tools strategically, in the information and cyber warfare domain. Many researchers have highlighted the misinterpretation and use of the term cyber warfare and information warfare interchangeably. This paper will first define and differentiate the differences between cyber warfare and information warfare. Then it will discuss the connection and the integration of this two warfare. Cyber warfare and information warfare have its challenges and posed threats to nation-states and the world. Knowledge and skills identified in information and cyber warfare will be discussed in this paper. In this regard, this paper will also discuss physical security and cybersecurity measures in addressing the threats posed by these warfare in this modern age.

I. INTRODUCTION

In this day and age, warfare does not only encompass the physical domain in areas of land, water, air, and space. Most countries around the globe are aware of the fifth domain, which is the cyberspace in their warfare doctrine and operations. This includes warfare attacks against a nation-state, destroying one’s critical communication channels, information systems infrastructure, and assets. Furthermore, in this complex world, physical and cyber warfare alone are insufficient. According to the 2019 Cyber Threat Outlook by Booz Allen, information warfare is one of the top cyber threats in 2019. Information warfare activities include an extensive range of tactics such as deception, spreading propaganda, and disinformation that are very important in warfare strategies. Information
warfare involve not only nation-states but individuals and organizations. Thus far, most countries only used information warfare for political and military purposes such as pushing voters’ decisions on their votes and fuelling cultural conflicts [1]. However, that might change soon due to the complexity of today’s environment.

II. THE SUBSTANTIAL DIFFERENCE BETWEEN CYBER WARFARE AND INFORMATION WARFARE

The idea and concept of cyber warfare are still new. The growth, commercialization, and high dependence of the internet and digital technology have boomed in the last two to three decades. Cyber warfare is politically motivated. It is an Internet-based conflict that involves attacks on a target’s information and system [5]. Another literature written by Peifer, Kenneth V. (1997) defines cyber warfare as “attacking and defending information and computer networks in the cyberspace, as well as denying an adversary’s ability to do the same.” Cyber warfare activities are all about but not limited to denial-of-service attacks (DoS), attacks on systems, malware attacks, ransomware attacks, system disruption, cyber sabotage, cyber terrorism, and attacks on the Critical National Information Infrastructure (CNII). Actors of cyber warfare can be nation-state, terrorist organization, criminal groups, etc. Actors are capable of carrying out cyber warfare attacks such as [6]:

i. Disrupting the telephone networks.
ii. Using logic bombs. A logic bomb is a malicious program that is set to be activated when a logical condition is met, on a certain time, date or after several transactions have been processed. The program can put the stock markets on a halt and destroy records of any transactions and money can be stolen by breaching the networks.
iii. Attacking a country’s power grids, which eventually will cause local dan regional blackouts. This had happened to countries such as Ukraine, Russia, Venezuela, etc.
iv. Causing malfunction and disabling computer systems, onboard avionic computers, or an aeroplane causing it to crash or collide.
v. Misrouting trains causing train crashes and collisions.
vi. Stealing of cryptocurrency or blockchain.

Cyber warfare cannot be separated or isolated from information security. To an organization and nation-state, information is the most valuable asset as it worth a lot of money. Thus, information security is essential and needs to be the top priority of an organization. Without information security, there will be a risk of vulnerabilities and possible threats and attacks to an organization. In general, information is always targeted for manipulation, deception, and espionage in information warfare.
Information warfare is not a new concept. Britain has manipulated information to change America’s opinion in 1917 and 1941 to engage in wars with Germany. On the other hand, in Germany, Paul Joseph Goebbels, known as The Minister of Propaganda, took over the national propaganda machinery that was responsible for creating the right image of the Nazi regime to its masses, which is the German citizens (Britannica). He continually makes press statements via the press and over the radio. He keeps raising hope to the masses, mentioning, and conjuring past events in history, as well as referring to some secret miracle weapons that the Nazis have in their grasp.

Both the United States (US) and the Soviet Union have been using broadcasting, the use of covert organizations and funds in their operations in order to intervene with other countries’ election during the Cold War [12]. Before the Internet exists, information warfare operations cost a lot of money due to training and movement of spies across borders. Nation-state at that time needs to establish foreign bank accounts and transfer of cash. In the present day, a nation-state remotely achieves a similar outcome at a lower cost. Rather than sending human agents, spyware and other internet tools are used to acquire, alter, and manipulate information across the globe. Funds can be transferred using cryptocurrency, which is harder to detect especially if it uses the tumbling services. Hence, technology and cyberspace easily execute information warfare operations faster, with less cost and low risk.

According to the US Department of Defence, information warfare is “an information-based attack that includes any unauthorized attempt to copy data, or directly alter data or instructions.” In a wider perspective, information warfare is not just about the involvement of computers and computer networks [17]. It is much bigger than that. The operation may involve different types of information transfer transmitted through any media which include the operations against information content, its supporting systems, as well as software. In addition, information warfare can involve physical hardware devices that stores the data, human habits, and practices as well as perceptions. This proves that the informational environment is brutal and war on itself.

According to the Joint Chiefs of Staff, information operations, which is also known as influence operations, is defined as the cohesive integration practice and engagement in the computer network operations, electronic warfare, psychological operations, military deception as well as the operation security. In information operation, tactical information regarding the adversaries is compiled and analysed. Furthermore, it is also used to create and disseminate propaganda in order to get a competitive advantage over the adversaries, competitors, or oppositions. There are three components to the information environment, which are the informational aspects, the physical
aspects, and the cognitive aspects of the environment [13].

- Physical environment aspect is where the individuals, organizations, information systems, and the physically connected networks reside.
- Cognitive environment aspect includes individual and collective consciousness, which information is used, and perception and decision are made.
- Information environment aspect is the intersection of the physical and cognitive domains which information content and flow exist, and a medium which information is collected, processed, and disseminated.

Information warfare activities are all about, but not limited to, psychological warfare, data and identity theft, electronic surveillance, intelligence analysis, public diplomacy, deception, disinformation, espionage, cyberbullying, and social media attacks. Using the social media to spread misinformation, can damage an organisation’s reputation or scrutinising and slandering government institutions and their policies. Social media can play the role to confuse the public, make the truth obscure and attack individuals, politicians, and organizations[1]. Information warfare via the social media confuses people and eventually disrupt social harmony and democracy. It will impact the country’s national security negatively. [5].

It is stated that the Russians are very skilful and the masters of information warfare ever since Stalin’s Rule of Supremacy. Stalin’s administration was very skilled in photo manipulation even before Photoshop existed. Stalin and his administration were notorious in rewriting the truth or even history through photographs. The Soviet photo engineers changed and erased faces of revolutionaries, enemies of the state, and other unwanted faces from official photographs so that it would not be recorded in history.

Stalin was famous for his Order 227 statement, which causes fear among the masses. Fear is considered a part of the information warfare. The contents of Order 227 circulated verbally to every single person in the army. The contents are required to be understood and memorised. Stalin, through Order 227, demanded and ordered that every officer, soldier, and political aides to understand that their resources are limitless, to fight until his/her death, and never to retreat. Cowards are unforgiven and were punished severely or even put to death. The laggards or deserters were drawn aside and shot without any reflection or remorse. Dr Martin Libicki in his seven forms of information warfare (shown in Table. 1) described that this kind of warfare contains the element of psychological structure in instilling fear to the troops. However, the elements of Order 227 have affected Stalin’s troops rather than the opposing force.
TABLE 1: Libicki’s Seven Forms of Information Warfare

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command-and-control</td>
<td>Disrupting the command effectiveness by attacking the command centres and the people in charge.</td>
</tr>
<tr>
<td>Intelligence-based</td>
<td>Reducing the opponent’s knowledge and awareness by increasing and equipping your own.</td>
</tr>
<tr>
<td>Electronic</td>
<td>Using cryptography and other tools to disrupt or halt the physical platform from transferring information such as network jamming.</td>
</tr>
<tr>
<td>Psychological</td>
<td>To play with the human mind and emotions. Can be used to demoralize or influence others.</td>
</tr>
<tr>
<td>Hacker</td>
<td>A hacker is a person that exploits the weaknesses and vulnerabilities of a network and computer systems. They find ways to breach security defences.</td>
</tr>
<tr>
<td>Economic information</td>
<td>In possession and in control of very important information which can lead to obtaining power.</td>
</tr>
<tr>
<td>Cyber</td>
<td>It can be a semantic attack, information terrorism, simulate-warfare, Gibson-warfare, etc.</td>
</tr>
</tbody>
</table>

Since then, Russia still has not lost its touch in information warfare. One of the recent information warfare incidents that involve Russia is about the 13 Russian officials who were caught meddling in the 2016 US Presidential election. They were charged on account of the conspiracy to deceive the US by ruining the functions of the Federal Election Commission, the US Department of Justice, and the US Department of State. They were charged with schemes to commit bank fraud, wired fraud, and aggravated identify theft (BBC News, 2018).

Another incident that has happened was the cyber warfare and information warfare activities against Ukraine by Russia. Russia has several times attacked Ukraine’s cyberspace, which includes attacks on its electricity grid, electronic billboard hack, influence their election and the integrity of their data [3] Russia tended to manipulate and fabricate stories and information to shock and caused international dialogue to be put into a halt.

The physical and cyber warfare increased due to global connectivity. Unlike any other nation-states, Russia sees the importance and the impact of information warfare, and they are very active in creating and spreading inflammatory rumours and exaggerate stories via the internet. This has caused a lot of problems for the US, NATO, and the EU. Russia tends to undermine the official version of events by using statements such as “Russia is a misunderstood and misjudged superpower and a necessary counterweight to Western liberal values. On the other hand, it is said that the western countries have experienced a deterioration of their ‘traditional values’ and has been hypcritical in their views and decisions in the international arena. As a result, Western philosophy, systems, and actions should not be trusted.” This is the perfect example of how information warfare is played in cyberspace.
Alternatively, at the end of 2018, Reuters reported that the Russian Internet search company Yandex was hacked by hackers working from Western intelligence. The hacker covertly maintains access to Yandex for at least several weeks without being detected. A rare type of malware called Regin was used to spy on the user accounts. Its architecture, complexity, and capability are on another level of advancement. Regin is known to be used by the “Five Eyes,” an intelligence-sharing alliance consists of countries from the US, Canada, Britain, Australia, and New Zealand. However, the intelligence agencies from these countries have refused to comment on the alliance. Yandex informed that the attack was fully neutralized before any damage is done, and no user data was compromised.

Other than Russia and the US, China has been seen investing more of their time, money and focus, on cyber and information operations, in conducting cyber espionage for political and economic purposes. China mostly targeted the US financial reserve and its defence industrial base. China wants to close the gap in knowledge, skills, and capability with its number one military rival.

III. THE INTEGRATION OF CYBER WARFARE AND INFORMATION WARFARE

Most countries see cyber warfare as a section of information warfare. However, in this technological age, whereby technology, as well as devices, are complex, sophisticated, and interconnected, the aspect of cyber is considered an essential tool in carrying out tasks including information warfare operations. Countries are now seeing cybersecurity as a critical issue. They are now setting up cyber commands and have developed or is currently developing national cybersecurity strategies to deal with the emerging cybersecurity threats [5]. A US Intelligence report in January 2017 suggests that 30 nation-states are developing cyber offensive capabilities. This reveals that cyber warfare and the cyber-arm race have already started to take root and will develop into something even bigger and dangerous [14].

However, having skills in weaponry, fighting, and cyber-attack capabilities are not enough in war situations. Perception management in information warfare is essential as the arms of war. Perception determines actors’ decisions and the next course of actions, especially on the battlefield. In this digital age, the public and the people worldwide are being sucked in and involved in the battleground. The society involvement in the battlefield is made clear and demonstrated during significant incidents such as the ‘Arab Spring’ demonstration in Arab countries and the ‘Jasmine Protest’ in China.

Another term for information warfare is information operations. The military uses the term as a tool for falsifying perception, and it is an integral part of cyber warfare. In cyber warfare, information is used for disseminating and spreading real and fake information. The military is able
to deny or stop access to information. Disinformation and fake news campaigns, as well as propaganda, can be used to deceive the enemy. It can influence public perception and trick them into believing or not believing a piece of information.

The rise and strong presence of the mass media have made governments realize the importance of perception management. Due to the advancement of the internet and digital technology, people are given opportunities to become actors, producers, and involved in information war via social media. The information spreads rapidly and sporadically than wild forest fires in this digital age.

In 2014, some intelligence groups acquire and even manipulate information via the internet. Other than affecting public opinion, information warfare has distorted information and make people believe what they want to believe. This information manipulation shows that there are high levels of decision making involved in the political arena. The manipulation of information and perception is already a lot and embedded in the cyber espionage, intelligence, and military operations, as well as destructive or disruptive cyber operations. The cyberwar information domain is significant for an organization or nation progress forward and achieve its goals [2].

Cyber warfare can be seen as defensive and offensive warfare. An effective cyber defence will be able to protect the network systems against cyber threats such as Denial of Service (DoS) attack, illegal access, cyber intrusion, network modification, or even jamming. It provides access to information, detects and identify the information systems, vulnerabilities and threats. It ensures that there will be an efficient use of the systems with less interference and disruption [2].

On the other hand, there are two functions of offensive cyber warfare. First is to identify, detect, manipulate, and affect an information system. Second is to disrupt or destroy the webbed information systems of adversaries. The attacker's process is reconnaissance, scanning, gaining access, maintaining access, and clearing tracks. With their knowledge, skills, and perseverance, they are able to conduct signal jamming, misleading information and malware, to alter, manipulate or wipe out important and confidential data of the opponent. They are able to congest the system with misleading information [2].

Recently, information warfare capabilities are more intense and widely used. Yet, cyber warfare is not merely a tool or a mode of executing information warfare, it is considered the primary mechanism to enhance information warfare manoeuvres. Attacks become more efficient, specific, faster to execute, in-depth, broader usage, and directly interconnected than in the past. Recently, there is a new information warfare on cyber warfare strategy, which involves hacking of the knowledge infrastructure (KI). For example, the spread of scandals, fake news and causing problems to an election-day logistics which puts the KI at risk. Some areas of concern on hacking knowledge infrastructure are in politics, finance, engineering,
Cyber-physical information infrastructure (CPII) has become a new target of cybercriminals. It involves heavily on the command and control of physical infrastructure. The critical national information infrastructures (CNII) sectors such as in Malaysia consist of Government service, defence and security, health service, emergency service, energy, water, banking and finance, food and agriculture, transportation, and information and communication, are frequent targets of cyber-attacks.

Following the targets of national knowledge industries, other targets that might be involved are institutions industries including education, engineering, surveillance, monitoring, investment, advertising, entertainment, and law. Knowledge hacking has progressed tremendously through time due to access and pathways that are easy to manage, and perimeters that can be breached.

Information warfare on cyber warfare is made possible by surrendering and ignoring the check and balance or counterbalance to the cyberspace ecosystem and conveniences. This shows that information warfare is trading security with convenience and not the other way around. The future of information warfare will consist of the combination of net warfare, electronic warfare, cyber warfare, and psychological operations. It will be widely used for offence attack and defence.

The combination of information warfare and cyber warfare use the ICT infrastructure to enhance and accelerate the movement of information. It will cover a wide range of audiences and with a significant impact on a nation-state or organization. Speakers or voice recordings are used in public or military operations to send or circulate a message more quickly and efficiently to the enemy combatants. The records usually aim to distract, confuse, and even anger the enemy combatants.

Another brilliant strategy that combines both the warfare is the use of social networks and targeted e-mail. These channels provide propagation of false information and disinformation by ambiguous people or false authority. The information does not need to be a total lie or part lie, as long as they can put a spin on the information and is able to distract the audience from the absolute truth.

Deception in terms of targets and sources can be used extensively via ICT. It speeds up the decision-making process and automates its consequences. Cyber warfare allows massive investigation on specific information such as a dossier on incidents, events, tendencies, and personalities needed to launch a successful information warfare operation. This is not always a contributing factor, but it can lead to a highly predictable response from the target population.
It is indisputable that the world has its focus on cyber warfare and information warfare. Countries such as the US, the United Kingdom (UK), China, South Korea and Australia NATO have set up dedicated cybersecurity centres to conduct these operations.

Cybersecurity experts in Malaysia have urged authorities to take cybersecurity and cyber warfare more seriously. Combating cyber threats and cyber attacks from nation-states can be very challenging. This is because some of these nation-states have no budgetary constraints in their cyber and information warfare operations.

An example of a state-sponsored cyber-attacks is an Advanced Persistent Threats (APTs) attack. APTs usually refer to cyber attack campaign that uses sophisticated hacking attempts. These attacks are usually persistent, continuously ongoing, and usually targeting an individual, organisation, or country. Their motivation varies from monetary, to cyber espionage, to obtain confidential data or even to spread misinformation, confusion, and chaos.

For instance, hackers from North Korea are more sophisticated as that are equipped with a wide range of knowledge and skills to conduct DoS, data theft, malware/ransomware attack and cyber espionage. The infamous 2016 $81 million cyber heists on the Bangladesh Central Bank were said to have been done by the North Korean hacking group, Lazarus. Hacking has become a handy tool for countries such as North Korea to acquire money and evade sanctions. This is especially useful when the sales of weapons and counterfeit notes are obstructed due to international restrictions.

However, APT attacks are not only executed by nation-states but also organisation or groups. The Carbanak syndicate has attacked banking, retail, hospitality, and other industry to obtain and collect financial information of the targets. The syndicate uses APT-style tactics to compromise their targets. Carbanak was able to employ and engage a commodity or leaked tools so that they are able to stop the abilities of the network defenders’ in identifying the Carbanak intrusions. So far, the syndicate is recorded to have stolen $1 billion from banks and other industries.

It is crucial to have a holistic and adaptive approach that identifies potential threats to organizations and impacts on national security and public well-being. Nation-states should look at the overall people, process, and technology of an organization and the nation-state. In addition, valuable data and information need to be protected by security with series layers of defence mechanism. This multi-layered approach helps to raise the security system from many different attack vectors.

It is essential to develop nations to become cyber reliance and to gain the capabilities to safeguard the interests of its reputation, image, brands, its stakeholders, and their value-creating activities. Nation-states should
implement a more proactive, dynamic, and integrated cybersecurity approach.

People are the weakest link in cybersecurity. Hence, there are two critical aspects of improvement to consider. First, everyone needs to be fully aware of their roles and functions in preventing and reducing cyber threats and cyber attacks. It is imperative to protect cybersecurity issues, risk, and gaps in the organization. Everyone has their responsibilities and roles in securing data and system in the organization. People need to realize that they cannot rely 100 per cent on security devices to prevent cyber attacks. Vulnerability and risk can happen due to human weaknesses. This can be from internal and external threats. Therefore, security awareness and training for employees must be one of the elements for improving cybersecurity in an organization. An effective security awareness program can reduce the risk of cyber threats that are aimed at exploiting people [6].

Second, the organization must recruit staffs specialized in cybersecurity. They continuously need to be well informed, updated with the latest knowledge, trends, skills, and qualifications to ensure appropriate controls, technologies, and best practices are implemented in order to handle current and upcoming cyber threats. All other employees must have knowledge on security, such as organization security policies, best practices in safety, guidelines, incident response and responsibility. Cyber resilience should be practiced throughout the organization. When security is in everybody’s mindset, the whole organization can predict, prevent, detect, and respond to the cyber-attacks.

Simulated cyber attack drill needs to be conducted annually or when needed. The drill needs to use the current potential cyber threats and cyber attacks. This is to create awareness and educate its employees with the anatomy of the attacks, to react according to Standard Operation Procedure (SOP) upon encounter. Time to time, cyber attack simulation or cyber drill on cyber attacks such as phishing, will minimize security risk in an organization.

Then there is the process. It is important to implement an effective cybersecurity strategy to identify ways organization’s activities, roles, and documentation are used to mitigate risks to the organization’s information. Due to drastic changes in cyber threats, the organisation needs to adapt and revise the processes timely. If people do not comply with the policies and processes, the organization is deemed inefficient.

It is important for organizations to prepare documented policy, processes, and procedures for their staff’s reference, handbook, knowledge, and awareness in handling vulnerabilities, threats, securing data, and cybersecurity. The policies must be in line with the standards and regulations that are currently implemented in the organization. These policies should comprise provisions related to internal and external workers. The workers are organisation staff, vendors, partners,
clients, stakeholders, and customers. The organisation must also regularly review and amend the documentation, guidelines, policies, and strategies such as the Risk Management Plan, Disaster Recovery Plan, and Business Continuity Management Plan to ensure the Cyber Security Life Cycles (Identity, Protect, Detect, Respond, Recover) are correctly implemented. Implementation of ISO/IEC 27001 in critical departments or units is highly advisable to implant the security mindset as daily routine and behaviour of the employees.

The business process in a cyber enabled space and technology is very important in order to tackle the risks and threats that occur in cyberspace. First, an organisation must identify their cyber risks, controls, and technologies needed. Technology is crucial to prevent, protect, or even reduce the impact of cyber risks depending on the organisation’s risk assessment according to an acceptable level of risk. Following are several examples of using Technology to manage cybersecurity:

i. Update software and hardware regularly.
ii. Remove unnecessary services and accounts.
iii. Enhance network security.
iv. Use encryption where necessary.
v. Update anti-virus programs.
vi. Identify existing risks and test controls.

Organizations must consistently identify and address risk through independent risk analysis and conduct security assessments as well as vulnerability testing to stop cyber-attacks. When an anomaly or weakness is detected, the system will raise a red flag. The details of the red flag are then shared with the relevant sectors. If the organisation’s system network and technology are properly maintained, the usage of information security controls are able to assist in identifying required protection for the task at hand.

In today’s complex digital age, cyber threat takes place across multiple layers. This is called defence in depth. Each layers of the organisation must have their own security defence and measures in order to cover all vulnerabilities. If they are not able to completely stop the attack, at least they are able to slow down attacks before damage is done. It is important for an organization to determine its critical assets, identify any vulnerabilities, and design security in their organization to prevent attacks and detect any breaches. The defence layers are physical, network, host, data, application, business process and organization strategy, and direction (as shown in Fig. 1).

In terms of managing and securing data, the government and organization need to implement confidentiality,
integrity, and availability in their documentation (CIA). Confidentiality limits access to information. The levels of confidentiality can be Top Secret, Secret, Confidential, Restricted, and Public. Meanwhile, integrity is to make sure that information at hand is accurate and has not been altered by any mean possible. Lastly is availability, which guarantees that relevant information or document are made available to authorized personnel.

Authentication is a method to authenticate a process to recognize and verify valid users or processes. It manages the information users or processes are allowed to access in the system. Whereas non-repudiation is the transparency and assurance that the information exchanges or any transaction may be trusted. It ensures that a party or a communication cannot deny the authenticity of their signature on information, document, or transaction.

Encryption is eminent and crucial to secure data. Encryption is installed and used in devices, computers, file servers, and across networks to assure the privacy of sensitive government, business, and personal information. Encryption technology is now a fundamental enabler for information assurance. It is available in the commercial marketplace throughout the world.

In addressing information warfare, the nation-state needs active transparency in its policies, capabilities, and activities. Transparency is considered a vital component for building trust and confidence between states bilaterally, regionally, and globally. Nevertheless, transparency is not the main aim, yet a toll for promoting further discussion on specific issues of national and international importance.

V. CONCLUSION

The threat of cyber warfare and information warfare is real and needs to be taken seriously. This situation worsens with the rapid spread of information technology, digital technology, and know-how, especially when both integrate or converge with each other. As more computers and devices are connected to networks for increased connectivity, vulnerability increased.

Through information technology advancement, the purpose of data based war in military activities will continue to develop, increase and in time evolve. However, it is a disadvantage to the less advanced nations. Most developed countries will take advantage of the less developed nation which impacted the loss of data, sovereignty, and system control.

This paper aims to provide a better understanding on the differences between information warfare and cyber warfare. It reveals the evolution of technology whereby information warfare and cyber warfare are linked to each other and utilized by nation-states to create a significant impact.

Nation-states and organizations need to develop a holistic and adaptive approach to prevent cyber
threats in cyber warfare and information warfare situations. Other than that, organizations need to implement multi-layered defence and implement innovative, dynamic, and knowledgeable cybersecurity approach against advanced cyber threats.

VI. ACKNOWLEDGEMENT

We like to express our appreciation to Col. Ts. Sazali Bin Sukardi (Retired), Senior Vice President, Strategic Research Division, CyberSecurity Malaysia for his pearl of wisdom and invaluable guidance in completing this conference paper. He is an expert in his field, which is cybersecurity and cyber warfare.

VII. REFERENCES


Cyberbullying via Social Media: Case Studies in Malaysia

Azriq Ariffin¹, Nurul Mohd², and Thurgeaswary Rokanatnam³
CyberSecurity Malaysia, Cyberjaya, Malaysia
¹azriq@cybersecurity.my, ²nurul@cybersecurity.my, ³thurgeas1197@yahoo.com

ARTICLE INFO

Article History
Received 06 Feb 2020
Received in revised form 13 Aug 2020
Accepted 8 Mar 2021

Keywords:
Cyberbullying; Social media; Cyber awareness; Safer internet

ABSTRACT

Cyberbullying is generally defined as employing electronic communication to bully or harass a person on the Internet, particularly on the social media sites. Advances in technology and better Internet access have enabled cyberbullies to find their way into the IT world. This paper presents two cyberbullying cases through the social media platforms in Malaysia involving suicide attempts. It highlights and presents a detailed discussion on the investigation and analysis process that reveals frightful and alarming facts on how social media are manipulated negatively which can lead to death. This paper also shares a learning module entitled the National Cybersecurity Awareness Module, an initiative by CyberSecurity Malaysia in ensuring safer Internet usage in Malaysia. The module consists of six topics including cyberbullying and is aimed at providing awareness and exposure to the need for safe conduct while using the social media. The suggestions and recommendations offered are towards ensuring a secure, resilient, and sustainable social media.

I. INTRODUCTION

The usage of the social media as a communication channel has grown tremendously and has become a necessity instead of a luxury. Anyone around the world who has access to the Internet has the potential to communicate with and attract a massive global audience. While there are many benefits to social media, such ubiquitous communication can also be used for negative purposes. For instance, cyberbullying has emerged as a potential harm with negative influence on the mental health.

Cyberbullying may have many serious and negative impacts on a person’s life and even lead to suicide. Harmful cyberbullying behaviour can include posting rumours, threats, sexual remarks, cyberstalking, trolling, flaming, sharing negative and false content, and denigration. As a result, cyberbullying victims may
experience low self-esteem, increased suicidal ideation and a variety of negative emotional responses, including being scared, frustrated, angry, and depressed.

II. RELATED WORKS

Cyberbullying has reached an alarming rate in Malaysia. The Star, one of the major newspapers in the country, based on a nationwide survey conducted, found that 8 out of 10 school children have experienced bullying in their schools [1]. Malaysia has seen some brutal physical bullying cases, such as the death of a 19-year-old schoolboy, T. Nhaveen, who was beaten up and sodomized by his former school bullies. Not to forget the death of navy cadet officer Zulfarhan Osman Zulkarnain, who was tortured and murdered by university mates over an allegedly stolen laptop [2]. Even though cyberbullying is done in the virtual world, the victims face consequences as real as those who suffer physically.

According to a survey conducted by the Malaysia Communications and Multimedia Commissions (MCMC) involving 14,000 school students, 70% of the respondents admitted to having been harassed online through improper pictures or messages posted and being called mean names [3]. Meanwhile, statistics provided by MyCERT (Malaysia Computer Emergency Response Team) of CyberSecurity Malaysia show that they received 260 reports on cyber harassment cases in 2019 [4].

III. METHODOLOGY

The analysis was conducted by reviewing existing literature on cyberbullying. Our goal was to examine whether the researchers had developed useful insight into this subject and to learn whether consensus agreement had already been reached on this subject. Based on our observations, we have found that there are several literatures focusing on cyberbullying. Most of the literatures reviewed are valuable in term of framing the contexts rather than directly providing a solution to the issues of this study. The materials reviewed include articles found on the websites, published conference materials, and referred publications.

The analysis was also done with reference to the Malaysia Cybersecurity Strategy 2020-2024 (MCSS). This strategy’s key objectives have been outlined in five (5) strategic pillars. This paper referred to pillar four (4) which aims to enhance capacity and capability building, awareness and education through three (3) strategic initiatives. Diagram 1 illustrate the pillars of MCSS which is one of the basis of this analysis.

![Diagram 1: The pillars of MCSS](image-url)
IV. FORMS OF CYBERBULLYING

There are many forms of cyberbullying discussed and referred to. Flaming, trolling, cyberstalking, denigration, harassment, masquerading, flooding, exclusion and outing are several types of cyberbullying that exist [5]. Based on a survey conducted by Statista, posting mean or hurtful comments online, spreading rumours about someone online, threatening to hurt someone via phone calls or texting, posting mean or hurtful pictures of someone online, creating mean or hurtful webpages about someone, and sharing racial or sexist remarks about someone online are among the most common types of cyberbullying identified [6].

The following table shows a list of cyberbullying and the definitions

<table>
<thead>
<tr>
<th>Type/form</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclusion</td>
<td>the act of leaving someone out of a situation deliberately. For example, a teenager being left out of message threads or group conversations that involve mutual friends.</td>
</tr>
<tr>
<td>Harassment</td>
<td>a general category into which many types of cyberbullying fall, but it mainly refers to a persistent pattern of mean and dangerous online messages sent with the intention of harming someone.</td>
</tr>
<tr>
<td>Outing/doxing</td>
<td>refers to openly revealing personal and sensitive details about someone without their consent. This is done solely to embarrass the victim on social media platforms by spreading personal photos or documents or sharing an individual’s personal messages.</td>
</tr>
<tr>
<td>Trickery</td>
<td>is similar to outing but involves deception. The bully will befriend the victim and try to gain their trust before abusing that trust by sharing the victim’s secrets and private information to third parties.</td>
</tr>
<tr>
<td>Cyberstalking</td>
<td>a severe form of cyberbullying that can go to the extent of physical harm threats, false accusations, and monitoring.</td>
</tr>
<tr>
<td>Fraping</td>
<td>when a bully uses a victim’s social networking accounts to post inappropriate content using their name. For example, someone may post racial/homophobic slurs through someone else’s online profile to ruin their reputation.</td>
</tr>
<tr>
<td>Masquerading</td>
<td>happens when a bully creates a made-up profile using a victim’s personal information and pictures.</td>
</tr>
<tr>
<td>Dissing</td>
<td>when the bully spreads bad information about the victim through public posts or private messages to ruin their reputation and relationships with other people.</td>
</tr>
<tr>
<td>Trolling</td>
<td>the act of bullying by intentionally posting</td>
</tr>
</tbody>
</table>
hurtful comments online to upset others. These bullies do not have a personal relationship with the victims.

| Flaming                  | is similar to trolling but involves more direct attacks on victims, provoking them into online fights. |

V. CASE STUDIES

A. Case 1

A recent case that has shocked Malaysians was that of a 16-year-old teenager who committed suicide after her Instagram followers voted in a poll that she should die. On 13th May 2019, Davia Emilia jumped to her death from a third-floor apartment in Batu Kawa New Township, Kuching, Sarawak. She posted an Instagram story earlier that day, around 3pm, asking her followers to choose whether she should live or die. The result showed 69% voted “D” that stands for “die” and the remaining voted “L” that means “live”. After returning from dinner at 8pm, her stepbrother found Davia lying lifeless below their rented unit. According to her neighbour, Davia was studious and always had a book with her whenever she was in a coffee shop nearby. She died 10 days before the mid-year school holiday started. Davia came from a broken family. A local news station reported that her depression originated when her father separated and remarried a Vietnamese woman in Singapore. It was also stated her father seldom visited her. On the other hand, her mother, an Indonesian woman, remarried a man with a 15-year-old son.

Earlier that evening when Davia died, her stepbrother invited her for dinner, but she refused. The city police chief added that Davia updated her Facebook status with “WANNA QUIT F***** LIFE I’M TIRED,” before adding it to her Instagram story. She also sent out a heartfelt WeChat status to her friends in Chinese later that day. After her death, Davia’s cousin posted a story on her Instagram account with “Just now you guys voted for “D” and this happened… Happy now?” (see Picture 1) [8].

According to MCMC, those who incited the 16-year-old girl in Sarawak to commit suicide based on the poll on her Instagram, may be liable under Section 305 of the Penal Code, which states that it is wrong to incite individuals aged below 18 to commit suicide.

B. Case 2

Another tragedy occurred in Penang when a young man jumped to his death from a flat after leaving a suicide note on Facebook (see Picture 2). On 2 May 2017, 20-year-old Teh Wen Chun, an engineering student,
jumped from the 17th floor flat in Tanjung Bungah, Georgetown, Penang. It was learnt that Teh had posted an apparent intention to commit suicide on his Facebook page prior to the incident. Wen Chun’s friends revealed that he was struggling with his studies and was under a lot of stress. He could not cope with the course he chose [9].

After his controversial death, a post on the TARUC Confessions-Penang Facebook page explained what happened to Wen Chun. The post made by an anonymous student said the victim was hurt by anonymous posts online. Wen Chun became depressed by an article that tarnished his image online. His friends did not notice his suffering until he revealed his intention to kill himself. Despite his friends’ effort to make him give up the idea of committing suicide, Wen Chun did it anyway. Wen Chun’s father, Ben Hock, told The Star Online he was aware of his son being bullied in the cyberspace. Wen Chun display change in behaviour when some of his college mates criticized and called him names on Facebook. The father added that Wen Chun said everything was fine and did not complain about the bullying. Ben Hock said his son probably could not handle the cyberbullying, which led to his suicide [10].

VI. INTERVENTION MEASURES

A. General measures

Victims can fight cyberbullying by taking certain measures like not responding to it. Striking back makes the victim become a bully as well. It is natural to want to fight back but stooping to the bully’s level to justify oneself is not a clever act. Children must seek an adult’s help, be it a parent, sibling, teacher or professional [11]. Another step that can be taken is to gather evidence of the bullying, such as online messages or posts sent by the bully. There are several non-governmental organizations willing to help children affected by cyberbullying like the Befrienders Malaysia and Penang Protect and Save the Children and the Women’s Centre for Change that offer helpline services. Cyberbullying can also be reported online by emailing to CyberSecurity Malaysia’s Cyber999 or using the mobile app available on Google Play and App Store [12].

Instagram too has taken certain corrective steps to curb cyberbullying. This application uses artificial intelligence (AI) technology to
minimize mean behaviours. The AI algorithms can detect potentially problematic content before it is posted and advises users of consequences that might arise. Instagram has also included a new feature called “Restrict” that allows users to block those who might post rude comments. A restricted user will not know that their comments will not be visible to other users. If the restricted user sends messages, these will automatically go into the spam folder of the message request inbox. The user can choose to either read or ignore the messages sent by the restricted user. The restrict feature allows the online relationship to continue but offers some controls of who and what can be seen. Users are also given the option to block someone to completely separate themselves from the individual. However, victims often prefer not to use this option because they are afraid of the bully’s reaction. Twitter has a similar feature for when individuals tweet or reply with hurtful comments [13].

Facebook gives the option to report inappropriate posts, comments, or pictures. The app has also set a few community standards it complies to, and it does not tolerate pages that identify and degrade individuals. Bullying photos and videos used to shame a victim, unwanted friend requests or messages targeted at other people, and sharing personal information to blackmail or harass other users are not acceptable. Snapchat does not tolerate bullying either. If an unwanted message or picture sent to a user indicates bullying or harassment, a report can be made by filling out an online form [14].

B. Signs of being cyberbullied

Everyone should always look out for certain symptoms in their children and people around if cyberbullying is suspected. The victim appears nervous whenever receiving texts, emails, or instant messages. Loss of appetite and being secretive or uneasy when asked about their social media life are also indications of cyberbullying [15]. Other classic signs are indulging in self-destructive behaviours, avoiding social activities, and loss of interest in education and sports [16]. Children might also have trouble sleeping at night or become frustrated after going online [17]. In some cases, parents are unfortunately the last ones to know that their child is a victim of cyberbullying.

C. National cybersecurity awareness module

CyberSAFE (Cyber Security Awareness for Everyone - www.cybersecurity.my) with the motto “Be Smart, Be Safe!” is CyberSecurity Malaysia's initiative to educate and enhance the general public’s awareness of the technological and social issues facing Internet users, and particularly the dangers of being online.

Through the CyberSAFE Program, CyberSecurity Malaysia has developed a National Cyber Security Awareness Module (NCSAM), which is a collaboration between CyberSecurity Malaysia and the Ministry of Education Malaysia.
through the Resource and Education Technology Division. In 2017, the idea emerged to develop an e-learning module based on a report for the National Baseline Study on Cyber Security Awareness among School Students in 2016 & 2017. The objectives of this module are:

i. To create awareness among school children.
ii. To be an alternative medium for teachers to teach ICT subjects with cybersecurity elements.
iii. To train “Briget Bestari” or Ambassadors to spread awareness messages among peers.
iv. To become content for Computer Club activities.

The target audience of this module includes school students aged seven (7) to 17. It also caters to special education and disability students. NCSAM consists of 6 topics:

i. Social Media
ii. Cyber Bullying
iii. Internet Safety
iv. Digital Citizenship
v. Balancing Time Online
vi. Online Ethics

The module has four (4) sub-modules based on the age or class as follows:

i. Sub Module 1: Cyber Bullying - Standard 1 to Standard 3 (Age 7 to 9)
ii. Sub Module 2: Cyber Bullying - Standard 4 to Standard 6 (Age 10 to 12)
iii. Sub Module 3: Cyber Bullying - Form 1 to Form 3 (Age 13 to 15)
iv. Sub Module 4: Cyber Bullying - Form 4 to Form 5 (Age 16 to 17)

Basically, on these topics, the participants discuss the definition of cyberbullying, differentiating between cyberbullying and bullying in real life, best practices to avoid being a victim, where to report, identifying the characteristics of victims, and the right things to do when children are facing bullying situations. The development of the modules started in 2018. Since then, the contents are being reviewed by the ministry and subject matter experts to make sure that they are up to date. In 2020, the modules undergo a pilot project at 300 schools in Malaysia to gather feedbacks from the ministry officers, teachers, and students. The inputs are used to improve the module and bring it up to standard in supporting the philosophy of the national education.

The module will be fully implemented in 2021. CyberSecurity Malaysia will collaborate with the Ministry of Education to ensure the successful implementation of the module towards achieving the objectives. It is hoped the module will help create awareness and also develop soft skills among students, especially for public speaking, and that it will become an influencer in terms of promoting information security and Internet safety.

Besides the development of NCSAM, a few activities are also in place to create awareness among
school children, especially on cyberbullying issues. The activities are:

i. CyberSAFE Awareness Talk. Talk on best practices, do's and don'ts, current threats, issues and creating awareness within 30 to 45 minutes.

ii. CyberSAFE Quest. Exploration/race game involving five (5) to six (6) checkpoints. Participants need to answer questions related to cyber safety before they can proceed to the next checkpoint.

iii. National ICT Security Discourse (NICTSeD). Students can sell their ideas and proposals on specific topics. This year is going to be the 8th year of NICTSeD and the participants are from secondary schools in Malaysia. Sixteen teams representing each state in Malaysia will be chosen to compete in the preliminary, quarter, semi and grand finals.

iv. Digital Content. Posters and videos on Internet safety and best practices for the various topics can be downloaded from the CyberSAFE Portal (www.cybersafe.my).

VII. CONCLUSION

The case studies shared in this article serve as real-life evidence of how impactful cyberbullying can be on someone’s life and even lead to death. With social media nowadays becoming the norm and most people having access to the Internet and smartphones, the risk is growing as anyone could become a victim of cyberbullying. Efforts from all parties such as families, friends and authorities are essential to educate and approach the intended audiences from both macro and micro-level perspectives. Control measures like those imposed by Instagram and Facebook show how serious cyberbullying is and that it needs to be contained. Prevention is better than the cure, hence, NCSAM was developed to help spread awareness among school children on various cybersecurity topics including cyberbullying. For a safer Internet via digital fluency fostering, mindfulness of how to be safe online and globally recognized etiquette ought to become second nature to Internet users.

VIII. REFERENCES


cyberbullying/ (accessed Dec. 31, 2019).
Establishment of a Method to Measure the Awareness of OIC-CERT Members

Tural Mammadov¹, Noraini Abdul Rahman², and Mohamad Farhan Mohd Rahimi
¹CERT Gov Azerbaijan, Baku, Azerbaijan
²CyberSecurity Malaysia. Kuala Lumpur, Malaysia
¹mammadov.t@cert.gov.az, ²noraini@cybersecurity.my

ARTICLE INFO

Article History
Received 01 Sep 2020
Received in revised form 16 Dec 2020
Accepted 08 Mar 2021

Keywords:
CERT, awareness test

ABSTRACT

Cyber threats and incidents have increased massively in the recent years thus it is very crucial in protecting and maintaining the critical infrastructures in organizations. The lack of awareness and active responses could be an issue to be highlighted for the Computer Emergency Response Teams (CERTs), which are responsible for incident handling process and mitigating the exposed risks faced by organizations and nations. Concerned about this, an effort had been made to strengthen awareness level among CERTs to improve the quality of services provided to secure and provide effective cyber security environment for the government and private sectors. This method also helps CERTs to exchange point of contacts, improve effectiveness of collaboration and built trust. In this paper, we proposed an awareness test to the OIC-CERT members which aimed to measure the level of awareness towards responding to incidents assigned to them correctly and in a timely manner. Three stages have been applied to ensure proper incident escalation are made to the team before the outcome being recorded from the respondents, respectively. The findings of this paper will provide an overview of the awareness level, check correctness and reliability of point of contacts, to build challenging environment to response tests on time and correctly and important lessons for the organizations to stay active and precise on the incident handling. On the other hand, the method needs to be improved to encourage the involvement of more respondents that will hopefully provide healthy cooperation among CERT members and getting a better, positive result.
I. INTRODUCTION

The Organization of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) consists of cyber security experts from Islamic countries that are responsible for the preparation, identification, recovery, and prevention in handling computer security incidents in their respective constituencies.

The OIC-CERT mitigate cyber threats or response towards incidents such as intrusions, malware, ransomware, and other malicious cyber activities including providing alerts and incident handling references. The OIC-CERT also conducts awareness programs, campaigns, and collaborations with its members in conducting research aimed at improving the level of knowledge related to the latest cybersecurity incidents.

These teams are working together in OIC-CERT to achieve the same goal of incident response. They respond to any computer security incidents with proper preparation including having complete security tools which is the key to a rapid response, identification and research process on the security incidents, recovery process where issue been handled and mitigated, removing threats and regaining control to pursue the system operational, and prevention phase to identify areas for improvement to avoid recurring issues.

In incident response operations, response time is a critical factor in the effectiveness of the process. In fact, hesitation in responding to incident can be damaging. It is important for the response team to keep the awareness level high, thus, this study was developed. It should also be mentioned that to keep awareness high is not to hurry without being attentive. In this test we will also test attentiveness to check if the incident handled in right way or not?! The main purpose in developing such system was to measure the awareness of the teams and encourage teams to be more active and accurate in incident handling and in cooperation. The OIC-CERT requires rapid and precise response to save time in the aftermath of an attack.

Some approaches have been carried out against the OIC-CERT teams for the purpose of the study. The first step is to collect the email addresses of the representatives from each OIC country team. The email address is used for the purpose of sending test links so that they can respond accordingly. The test results are recorded based on the time taken to respond and how correct the response is. The key elements of the test were the time taken and the accuracy of an incident response team in ensuring a productive and effective response.

Implementing the following study and recommendations should facilitate efficiency and effectiveness of incident response for OIC-CERT.
II. RELATED WORK

A. Computer Emergency Response Team (CERT)

CERT is an organization devoted to ensuring that appropriate technology and system management practices are used to resist attacks on networked systems, to limit damages and to ensure continuity of critical services despite successful attacks, accidents, or failures [1].

CERTs are also known as the Computer Security Incident Response Teams (CSIRTs) in some constituencies. They operate in various sectors such as academic, commercial, critical infrastructure, government, military, and business, among others. However, the special kind of CERT is the national CERTs that operate at the national level and act as a security point of contact for the country [1].

In the other hand, NIRT is also another term of CERT, known as the National Incident Response Team of NCSC (National Cyber Security Centre). The primary aim of the NIRT assistance in crisis situations is to support the company to recover the essential services and business processes of the victim or organizations [2].

The CERT (Computer Emergency Response Team) operation of the NCSC-FI (National Cyber Security Centre - Finland) takes care of the prevention, investigation, and communication tasks in case of information security breaches. The main purpose of the CERT operation is to produce and maintain the cyber situation awareness together with domestic and foreign partners and counterparts. As an essential part of the CERT operation, the NCSC-FI acts as a national point of contact for information security breaches and threats. It also investigates these cases and helps the concerned parties [4].

Computer Emergency Response Teams (CERT) should be established to improve the security cognizance among people. CERT can also help establish new cybercrime laws, train computer forensic teams, and support organizations and users in fighting cybercrime [5].

The establishment of the Computer Emergency Response Teams (CERT) is one of the initiatives to reduce and mitigate cyber threats. [6]

B. Awareness Test

An attempt was made by a previous study to explore and figure out the local community present weakness facing a cybercrime threat. The motivation for this study was to examine the current awareness skills among the students and local community and help them in how to secure their privacy, services, and smart devices. An online and printed questionnaire was distributed for the participants in Bisha University in Alnamas District. One hundred thirty-five subjects were randomly selected, and all completed the protocol test [3].

The questionnaire sheet was based on the 2nd International Conference
on Anti-Cybercrimes (ICACC 2017) ideas, and provided a good survey that enables the authors to address the community’s awareness and the lack for both an effective anti-cybercrime training courses for strengthening the local community resilience facing such technology crimes; and a good survey, enables authors to address the current needs in using current technology-based services, systems, and applications [3].

The results proved that building a safe and a secure community requires, both governmental and non-governmental institutions to share and integrate their responsibilities and efforts against the growing cybercrimes. It is quite clear that, a legal awareness is very low rate (33%). Also, a cybercrime’s knowledge metric gives low rate (38%). Comparing a national anti-cybercrime system versus a global anti- cybercrime system, the study alarms the national institutions to be close to a community for handling cybercrime issue [3].

The study concludes that, the levels of the participants’ knowledge in dealing with cybercrime issues and threats is very weak. The lack of security knowledge against a cybercrime risks is quite high. It is noticed that there is a lack of awareness on cybercrime risks, and there is strong desire to receive an anti-cybercrime training and support. In comparing the study results with the previously related studies in literature review in the region, this study gives a good awareness on cybercrimes threats in this area. Future direction can be performed in several areas. The first area would be expanding the number of input parameters in the dataset. The second area would be feature extraction on input variables to cover online awareness aspects. Also, a set of prediction algorithms can be used to predict cybercrime risks [3].

One of the best ways to make sure company employees will not make costly errors regarding information security is to institute companywide security awareness training initiatives that include but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters [5].

The Government of Malaysia has been aware of the need for greater awareness and understanding of cybersecurity issues and for developing a positive cybersecurity culture [6].

A study entitled National Strategy for Cyber Security Acculturation and Capacity Building was carried out in 2010 to evaluate current national and CNII awareness education programs and campaigns [6].

To ensure the success of the cybersecurity awareness, acculturation and education programs, coordinated initiatives and efforts have been driven by relevant organizations to increase the level of cybersecurity awareness, best practices and safe use of the Internet across all CNII (Critical National Information Infrastructure) as well as public elements [6].

The National Security Council of Malaysia, with Cybersecurity Malaysia as the technical expert
agency, have co-organized a periodic national cyber crisis entitled X-Maya since 2008. The main objective of the drill is to exercise the workability of the National Cyber Security Response, Communication and Coordination Procedure and to raise awareness of the national security impact associated with the significant cyber incidents among CNII [6].

Securing CNII against cyber threat activities requires the efforts of the entire nation. The government alone cannot sufficiently secure the CNII. It calls for a public-private-community cooperation in addressing the matter. The government can take the lead in many of these efforts, provided it is supported by the private and community sectors [6].

Focusing on the technical task of the incident response team, the use of the right technical tools that support the work methods can greatly increase the effectiveness of CSIRTs. The effectiveness may lie in the field of lead time of solving the incident, on the financial level and on increasing team knowledge and shared situation awareness within the CSIRT [7].

The initial assessment of the size and risk of a specific cyber security incident is ascertained on an ad hoc basis and is predominantly based on the knowledge level of the CSIRT team member who first gets the incident reported [7].

The CSIRT’s success depends on many factors, such as the technical resources at their disposal and team members’ level of knowledge and skills. In addition to these factors, a team’s success also depends strongly on the participation and cooperation of individual CSIRT members and other individuals, teams, and departments within and outside the organization [7].

Hence, teamwork is of the utmost importance in incident handling. Teams have the potential to offer greater adaptability, productivity, information processing capacity, and creativity than any one individual can offer. Moreover, teamwork is vital to transforming individual members’ disparate incident knowledge into a shared awareness of the evolving situation [7].

III. METHODOLOGY

The implementation and measurement on the effectiveness of the method can be divided into several stages.

The initial stage is about gathering the emails of the PoC member teams which will participate in the tests. The email addresses include representatives from the OIC-CERT. A valid email address is needed from each of the representatives to ensure the test link is being sent.

The second stage is about sending emails with a unique test link to each team to measure the response time of the teams. The time will be measured automatically and each team after clicking will see his/her response time and response rate. The Administrator will share the general response time and rating list for all teams after each test.
The last stage is to improve the test scenarios to harden the requirements and test skills of team members with real incident scenarios. It is important to ensure that the measurement is not only how quick the time taken for the teams to respond to the incidents, but it is also important to analyse how correct the teams act instead of to respond incidents or tickets opened to them. This approach will train the teams to respond rapidly and attentively, in order to correctly handle the required tickets or incidents.

IV. ANALYSIS AND RESULTS

The latest result on 11th March 2020 shows the highest difference in the gap between the responding participants and the non-responding participants which is 21 people. This issue occurs due to two identified factors which are no response from the respondent, and email addresses that do not work or do not reach the recipient. The percentage for teams who respond quickly and correctly will be affected negatively if the number of respondents continues to decrease over time.

Figure 1 above illustrates the OIC-CERT Team Awareness Test statistics recorded from October 2019 to March 2020.

According to Figure 1, there are upward and downward trends in the response recorded respectively on two variables. The responding team decreases steadily in the number of respondents during the test period conducted. The unresponsive team shows an increase in the number of non-responses over time.

As the number of respondents decreases during the test period, the quantity of teams that responded correctly on the incident or tickets opened to them certainly shows a small number.

Figure 2 shows the measurement of the awareness test’s effectiveness, including the problem encountered during the test. The number of correct responses on the first two test dates shows a lower amount than the incorrect responses. However, the correct responses on 6th February and
11th March 2020 shows a positively higher result than the number of incorrect responses. The result indicates the successfulness of the team that managed to respond accordingly to the main purpose of this test.

Figure 2 also illustrates the rising amount of unresponsive team over time showing a large gap compared to the responded team. Apart from that, the undeliverable emails displayed in the figure also affected the outcome of this test, even though came out with very small numbers.

These teams can be classified as undergoing this test successfully coinciding with the main purpose of this test being conducted. These teams have shown the positive level of awareness and encouragement to be more active in incident handling and in cooperation.

Based on Figure 3, the quickest response was logged from the Libya-CERT in recording 0 minute to respond the test correctly on 11th March 2020. On average, the above analysis displays that the time taken to obtain the correct response is less than one day.

After some tests, we revealed some issues that not only to get better results, but also, we need to get OIC-CERT corporation and information exchanges to be effective. They are:

1. The responses of the teams is not good enough as some teams do not respond at all.
2. With the tests it is possible to reveal that some teams’ emails are not working properly or not getting emails which is not normal for the PoC contacts as they are used for communications and other purposes.
3. The teams’ information and contact details need to be updated and controlled on a regular basis.

Pursuant to the issues listed above it was decided to have a system for member teams that will require the teams to update contact details and Point of Contact (PoC) information by themselves on a regular basis such as automatic update of the member’s
data. This will assist the process as follows:

- All member teams’ data to be up to date.
- All member teams’ information and point of contacts will be available to all member teams.
- It will help to shake “sleeping” teams with alerts and push messages and encourage them to be active as well by updating team information and participate in information exchange on a regular basis (once a quarter).
- It will help the secretariat to activate and involve those inactive teams in activities within the OIC-CERT.
- It will automate the registration of new members.
- It will give opportunity to hold online voting for the new members.

All the above mentioned items motivated us to create another system where we can handle all those issues and integrate the awareness algorithm as a subsystem. It will give us opportunity to do a test on fully operational and complete system, measuring the awareness of teams and generating automatic statistics and so on.

V. DISCUSSION

A general finding from the awareness test system of OIC-CERT members is that the number of respondents throughout the period are still small in numbers and decreasing. Instead, the number of the non-responses has shown an increased in numbers. It is important to ensure that the teams email addresses are reachable and ensure the teams cooperate accordingly to this test.

The support from the teams will ensure the real overview of the study to get better result of the overall participation. Apart from that, the positive outcome corresponds with the objective of this system as some of the teams have successfully responded to the incidents correctly in a timely manner. The result complied with the aim of the study to measure the effectiveness of the system to indicate not only how quick the teams responded the incidents, but also how correct they acted to the task.

Some improvements can be done in the future to increase the involvement of the participants. The PoCs need to be updated from time to time to ensure the participants receive the required test links. It is recommended to use the automatic update of the member’s data to ease the process of the system onwards.

Apart from that, the team needs to improve on responding to incidents such as the need for better tools in support of teamwork. Alternatively, it may be due to the resistance to change in the way the teams have always worked, for example when it comes to use tools to estimate size and risk of an incident. This was always done based on team members’ skills and experiences with similar incidents and there is no obvious need to do things differently [7].
VI. CONCLUSION

This study was conducted among OIC-CERT members in a same, particular period with unique test link via email delivery. The delivery time was selected so that the email delivery time to be the working time of all members around the world. It was 13.00 GMT+4. Another thing considered was that the response time of each team calculated according to email delivery time – response time. Where it means email delivery time was unique for each team as the system is sending the emails with the pause not secure itself not to stuck in spam filters. The results conclude that the highest record registered (60%) is from the no response attribute, excluding about (3%) of undelivered emails and it is noticed that there is a lack of awareness for incident response. There is about (37%) of commitment from several teams that successfully responded to the test, including about (10%) teams that correctly react to the incident in a timely manner, were recorded. This study gives a good awareness for OIC-CERT members in actively mitigating cyber security incidents with proper incident management and rapid handling.

Future improvements and considerations can be made in several areas. The main aspect is to enhance the initiative in obtaining and updating the newest PoCs from the members involved, especially representatives from OIC-CERT. Second, ensuring the involvement and participation of all participants involved in this test to obtain more accurate test results. Also, highlight the objectives and purpose of the test performed to measure the time taken and the accuracy of participants in dealing with incidents.

VII. ACKNOWLEDGEMENT

We would like to thank members of OIC-CERT for participating in the awareness test and contributing the publication of this paper.

VIII. REFERENCES


Talent development in the area of cyber security rapidly evolve due to the dramatic changes in cyber threats and attacks. The needs of professional certification in cybersecurity industry have been addressed by many organizations throughout the world. It was reported by many sources, there is an exponential growth in the demand for cybersecurity professional and special treatment for employee with professional certification. Malaysia encouraged cybersecurity graduates to obtain professional certification for better employment. Malaysia Higher Education Blueprint stated that future ready curriculum includes certificate ready academic program. It is believed that this model can increase competency, knowledge and skills among university graduates. Therefore, rapid growth of cybersecurity professional examinations at the global level which are product-oriented scheme can be seen. There were limited studies that explored the advantages in obtaining certified cybersecurity professional. To our knowledge, none of the previous research shared the best practices for assessment procedure in professional cybersecurity competency modules. This article presents the method in handling examination for Cybersecurity Professional Examination by adopting ISMS generic pillars known as People, Process and Technology. Our framework consists five (5) main components structured in a loop. The five modules are examination question development, examination system, examination conduct, results coordination and manuscript management. As a conclusion, professional examinations must undergo a proper process to make sure it complies with international standards and penetrate the global market.
I. INTRODUCTION

Competent-based education has gained attention recently. This is due to the demand for high skilled workers in many countries around the world. High skilled workers can be measured through experience, career profile, educations and certification received [3]. Cybersecurity professionals is referred to a person who works in cybersecurity industries and certified to special area in security and related field. To be certified, the person is required to sit for professional exam which is totally different from formal bachelor’s degree education. Many studies were conducted to investigate the best model for assessing skills and knowledge in the areas of medical and health but none of the studies explore the methods used to assess skills in cybersecurity. This article presents a framework for conducting assessment for cybersecurity professional competency. It is structured in five sections which covers related work, methodology, implementation, discussion and conclusion.

II. RELATED WORK

The Certified Information Systems Security Professional (CISSP) that is currently organized by ISC² originated from Hongkong. Meanwhile the Computing Technology Industry Association (CompTIA) is a company introduced computer security professional examination with the emphasis on network and awareness. Cisco security focus on Cisco products and the very recent technology.

The Global ACE scheme does not rely on product; it addressed four main components: people, process, procedure and technology.

III. METHODOLOGY

The Information Security Management System (ISMS) has three pillars which are people, process and technology. To be robust, information security implementers and practitioners will make sure the system used complies with the requirements of the International Organization for Standardization (ISO) standards.

Framework development comprises four major process structured in a loop: first Examination Setting, second Examination Question Development, third Examination System & Development & Maintenance, fourth results coordination. The final module is Manuscript management which includes disposal & archive. Each module is built with a working process. Figure 1.0. depicts the process flow for examination for professional certification.
We developed a few important entities in module one i.e., examination setting. The entities are people, process and technology. People are the committee for examination management. The process and policy cover operational flow for the exam and technology refers to system used for the examination centre.

A. Mapping Component

The ISMS pillars comprise of people, process and technology [1]. In our framework, we defined people as the governance authority that is designed to control the quality of the professional certification and sets directions. Under process, our framework classified all modules as the process that are required to execute the examination plan. Technology refers to system. Our examination system is online, intelligent and interactive. The following sub section explain each component with its respective roles.

B. People

Several committees are involved in the people component of the pillar. They are: Board of Governance, Professional Examination Committee, Course Development Committee and the Subject Matter Expert (SME). All committees are assigned with special terms of reference. Examination secretariates are responsible to administer the overall process in the framework.

The Professional Examination Committee (PEC) is responsible for the governance of the examination process framework from the start to the end. The Board of Governance (BOG) is responsible for the overall process and issues in the scheme. The BOG has the full power to award certificates to the candidates who passed the examination. The third committee is the Course Development Committee, which is a working group that develops training content. This committee is important as a point of reference to the question developers. A Subject Matter Expert (SME) is an individual or group that is assigned to develop the examination questions.

C. Process and Policy

This part addresses operational issue which starts with examination manual development, call for questions, question development, vetting, compliance audit and results & appeal. The process is complied with standards ISO17024:2012 Conformity assessment — General
requirements for bodies operating certification of persons.

What make it different with normal examination procedure is that, the question development must comply with competency examination standards. The failure to follow the standards will result in non-compliance with certification and competency.

The professional examination should align with three components in the competency model i.e., knowledge, skill and attitude (KSA).

D. Technology

The examination is conducted online at an examination centre appointed by an authorized body. One of the criteria is that the centre is able to provide a room that has computers that can run the examination portal. The Education Management System for professional examination competency scheme must be equipped with modules that automates operations set for conducting examination. These include questions bank, random function, marking facilities and result analysis. Intelligent elements must be embedded in all functions. In addition, the system needs to be highly secured.

IV. IMPLEMENTATION

The proposed framework implemented under the professional cybersecurity competency scheme named as Global Accredited Cybersecurity Education Certification Scheme or Global ACE Certification Scheme. The Scheme was developed by CyberSecurity Malaysia and supported by industries and academics in related fields.

The scheme provides professional cybersecurity training in three levels: fundamental, intermediate and specialisation and professional certification. The certification shall be awarded to the candidates who passed the respective professional certification examination.

A. Question Development

The professional examination framework was implemented to the scheme since 2016. Each scheme requires examination and call for questions for each scheme are given to a dedicated group termed as Subject Matter Experts or (SME). Each module is executed with the standard operating procedures and governed by the Professional Examination Committee (PEC).

The continuous quality of improvement for overall examinations process which covered the scripts for questions, the process and results approval must comply with the professional examination standard controlled by the Quality Committee.

A call for questions script is requested quarterly. All subject matter experts presented their proposed scripts for questions irrespective to scheme. Vetting process will be conducted consequently, and selected questions will be transferred to a question bank. All questions must go through a vetting process to make sure it
complies with the KSA descriptor. The question developer has to make sure all requirements are fulfilled before submission.

The Professional Examination Committee are also responsible for examination system. The system is controlled by examination centre authorized by Cybersecurity Malaysia. All criteria are set by Cybersecurity Malaysia and the Board of Governance (BoG) of the scheme. Any organization or company could apply to be an examination centre if they fulfilled the required criteria. Cybersecurity Malaysia may withdraw the appointment as examination centre to any authorized centre with valid reasons. All regulations are documented in the Examination SOP.

B. Examination Conduct

The examination system allows all candidate to seat for online session. The multiple-choice questions are inserted to question bank and the system executed on the examination day. The examination centre will provide an examination hall which consists of controlled computers connected to protected examination portal. Candidates are asked to enter the examination laboratory fifteen minutes before Global Accredited Cybersecurity Education examination starts. User login and password are used as the control mechanism. Once login the candidate can only access the examination portal and all other applications are locked. Candidate are asked to read questions and select best answer from lists of options. It is a multiple-choice question. Once the candidates completed the examination, they can leave the hall and the results will be released approximately two weeks after the examination.

C. Results and Appeal

The result is generated by the system and only can be released after being approved by the Professional Examination Committee. Those who failed in the examination can apply for appeal in the next session.

The final process is archive. All used questions are not allowed to be reused or recycled. Within certain period the questions need to be removed from the system and it is termed as archive.

V. DISCUSSION

Cybersecurity competency is in demand. Professional certification in cybersecurity which available in the market are mostly product oriented. The complete process of certification consists of four major operations which are membership, training, examination and certification award. Certifications are categorized according to three levels: foundation, intermediate and advanced. Each level has different types of competencies which comprises of knowledge, skill and attitude.

VI. CONCLUSION

The Global ACE Scheme framework are mapped with the pillars in ISMS which are people, process and technology. The proposed
examination framework is aligned with Competent Based Education model (CBE) that are widely used for technical and vocational education (TVET).

This study presented best the practice in establishing professional certification for cybersecurity to support industry need and competent based education towards future-proof curriculum. The framework complies with ISO 17024 and it brings the GLOBAL ACE scheme accepted worldwide.

This article brings insightful information for practitioners and educators who is going to develop cybersecurity competency certification.

VII. ACKNOWLEDGEMENT

We would like to express our gratitude to Universiti Teknikal Malaysia Melaka and Cybersecurity Malaysia for supporting the Global ACE Certification Scheme.

VIII. REFERENCES


Overview of Prioritization Model for National Critical Sectors Protection

Ariani\textsuperscript{1} and Muhammad Salman\textsuperscript{2}
\textsuperscript{1,2}Electrical Engineering, Universitas Indonesia, Depok, Indonesia
\textsuperscript{1}arianitkj2@gmail.com, \textsuperscript{2}muhammad.salman@ui.ac.id

\vspace{1em}

\textbf{ARTICLE INFO}

\textit{Article History}
Received 21 Oct 2020
Received in revised form 11 Jan 2021
Accepted 08 Mar 2021

\textbf{Keywords:}
critical sectors, protection, prioritizing response, service level agreement, security monitoring;

\textbf{ABSTRACT}

The national critical sectors are an important sector that should be paramount in maintaining the state security when cybersecurity incident occurs. The national critical sectors aim to secure facilities, networks, information and physical assets. Protection against national criticality involves protection of both physical and cyber components, where cyber protection plan must be included in the national defense strategy. This article aims to propose a design of prioritizing model as early detection of cyber incidents as part of managing the incident and protecting the national critical sector.

\vspace{1em}

\textbf{I. INTRODUCTION}

Cyber-attacks or other undesirable cybersecurity incidents can cause disruption to our daily life. The impact of cybersecurity is one of the challenges in public life and even a challenge for the national defense of a state or country, thus it is required to have a cybersecurity strategy to be part of a protection plan program \cite{1} to protect the national assets.

Since World War II, safeguarding national resources and assets have become part of national defense planning. Along with cyberspace development, the national defense's perception has begun to pay attention to securing information and physical-based facilities, networks, and assets \cite{2}. Regner et al. stated that a country must define priorities, objectives, goals, and scope which cover cyberspace, cyber governance, cyber defense, cybersecurity, and cybercrime when designing a national strategy \cite{3}.

Important components related to this domain are cyber policy and cyber governance- that useful as national instruments to regulate and protect cyberspace. One of the regulations, which is noteworthy as national defense, defines critical sectors that become the most priority.

The definition of critical sectors are a sector group that must be protected as a top priority when an

\vspace{1em}

\textbf{ISSN 2636-9680}
eISSN 2682-9266
incident occurs because its impact can lead to the collapse of a country. Critical sectors are sectors that have not only strategic infrastructure but also strategic information.

Therefore, it is important to focus on proactive steps to build the resilience of individuals, organizations, and countries against security threats such as cybersecurity capacity. One focus area is incident management and response, scoping on responding to the security incident and protecting infrastructure [4]. Enisa [5] stated that the national cybersecurity agencies, who have led the role of protection cybersecurity needed to the critical sectors (they have called it critical infrastructure), aim to provide the support for automated-prioritized handling of incidents affecting. So, the incidents that involve critical network assets are notified automatically, and the handling is prioritized.

Related to the protection infrastructure, NIST develops a framework to identify prioritized, flexible, repeatable, performance-based, and cost-effective approaches, including information security measures and controls. It can be adopted by other organizations [6]. One of the core frameworks is "detect", which makes it possible to indicate events that threaten cybersecurity. Examples of implementation within this function include Anomalies and Events; Security Monitoring; and Detection Processes.

Among the incredible number of events detected by detection tools like security monitoring, the handle response is considered the Service Level Agreement (SLA) management and security management. From a business perspective, the SLA aims to offer agreement between the users and the Service Provider, and it is to establish what is effectively granted in terms of quality [6]. From a defense perspective, SLA means the severity level on response prioritizing incidents that occurred.

The relationship between the national defense strategy in protecting critical sectors with response prioritizing incidents is how to design plans and programs specially made to protect the national critical sector security. A comprehensive design is needed to secure the critical sectors from a cyber perspective.

II. RELATED WORK

In [7], the authors have proposed SLA Mapping to be one part of the design SLA based on workflow management on intrusion tolerance with case cloud computing service. Jusas et al. [8] have proposed a logical filter to attack detection. They have said that the general classification of cyber-attacks includes the stage of the cyber kill chain, type attack, and target attack (object groups, state institutions, economic branches, social, etc.). So, the prioritizing an incident must pay attention to them, and the variable related to national cyber defense is the targeted attack.

Spring et al. [9] have proposed prioritizing vulnerability response specific to vulnerability categorization that occurs to stakeholders. The national sector's diversity must accommodate the primary function of handling rather than being included in optional features that are difficult to use.

In [10] [11], they have proposed a method to define an alert intrusion detection system's response as
severity level selected, which focuses on target anomaly. It gives specific results for each event category when describing suspicious activities one type of suspicious event.

Bernieri et al. [12] have researched decision making method on intrusion detection as protection tools of critical infrastructure. The method used is based on Analytic Hierarchy Process (AHP). Their experiment identified the highlight of the methodology that have designed for the decision support. Wang et al. [13] have proposed risk decision-making theory to prioritize incidents by minimizing the sum of business losses and risks. Imamverdiyev [14], Al-Subhi [15], and Berinjan [16] used Fuzzy decision making to prioritizing the incident, but without specific indicators. Another research was conducted by Dileep Kumar Singh [17]. He has implemented multicultural decision making using the ELECTRE method. Research on the priority of incidents was also had carried out by Renners et al. since 2017 [18].

They determine priority incidents by prioritizing rules with a tree model. In 2019, Renners et al. [19] modelled priority incidents by determining policies that have set rules and derived attributes; this policy is based on adaptive learning. Adaptive learning is used to enable an analyst to formulate feedback on incident responses. In [20] [21], Anuar et al have proposed incident prioritization using the Analytic Hierarchy Process (AHP) method and Risk Index Model. Furthermore, they have made detailed indicators that must be considered in determining priority incidents.

III. PROPOSED APPROACH

Our approach's baseline is first to find a prioritization mechanism for the security monitoring setup that has been researched by the researcher. It will give insights into the expected efficiency of proposed strategies to setup security monitoring. We could propose a design for automatically computing the prioritized result out of SLA mapping from these insights. The proposed prioritization model is illustrated in Fig. 1.

The first focus study defines severity by calculating features for indicator needed, which it could be customized on the feature of security monitoring. The next stage, mapping the sectors, which is defined as the national critical sectors. Then, the decision-making method needs research in-depth applicable to the real environment.
A. Security Monitoring

The security monitoring system is a system used to secure infrastructure, usually using an intrusion detection system. The security monitoring system provides information in the form of logs and activities that occur on the network. Several security monitoring systems offer the anomaly category that an anomaly occurs, and the SLA system is automatically generated.

B. Defining Features Score

The next phase is defining the severity score by calculating features. This method was adopted from a previous research [10], which used this stage to get the score of each variable generated by the monitoring system's features by calculating the features into a formula to determine the response based on the average feature score. Every feature has a type of indicator which is defined by review of some research. In addition, these indicators are classified into 2 types- urgent and critical- which are displayed in TABLE 1 and it is illustrated in Fig. 2. Each indicator will be calculated by the appropriate formula.

<table>
<thead>
<tr>
<th>No.</th>
<th>Critical</th>
<th>Urgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Criticality</td>
<td>Severity</td>
</tr>
<tr>
<td>2</td>
<td>Maintainability</td>
<td>Exploitability</td>
</tr>
<tr>
<td>3</td>
<td>Replace-ability</td>
<td>Similarity</td>
</tr>
<tr>
<td>4</td>
<td>Dependability</td>
<td>Sensitivity</td>
</tr>
<tr>
<td>5</td>
<td>Control</td>
<td>Frequency</td>
</tr>
<tr>
<td>6</td>
<td>Impact(CIA)</td>
<td>Vulnerability</td>
</tr>
</tbody>
</table>
The critical type refers to a comparative state in which one incident is very important because of impacts are the three main attributes that are common in security, such as confidentiality, integrity, and availability (CIA). The Urgent type refers to circumstances where one incident requires a quick response compared to other incidents based on the possibility of threats and vulnerabilities.

Research and experiment have been done for this phase. It shows that the priority setting phase produces more detailed information in defining if the same event is a priority or not due to different feature scores. Priority responses given can differ depending on the most impact on the network so that it is quite sufficient to be applied with the response model.

C. SLA Mapping

The SLA Mapping is a service level agreement that is defining as important and prioritizing the critical sectors. The intension of protecting among the national defense by secure the government's critical sectors is defined. Those sectors list could be customized depending on the country regulation.

D. Decision-Making Method

The next process is the decision-making method as an algorithm or science method to give a decisive response. The method uses a decision-making algorithm because it does not need a learning process by training data. And lastly, after all the processes above, the result is a response selected as a service level handling incident. So, the incident handler can choose which the incident must be responded.

E. Discussion and Limitation

Each phase of prioritizing design to determine the service level agreement's response is important to determine effectiveness in analyzing a suspicious anomaly found in the monitoring system. Effective incident management provides benefits that allow an incident to be handled quickly under the appropriate time frame and handling process before the incident has a more significant impact. In this way, we can minimize the target's impact, especially national critical sectors, with good management visibility.

The proposed approach's focus is the design to determine the priority response of service level agreement, where the priority response is one of the incident management processes, triage incident. Although during our study, it did not evaluate all stages of the proposed design. However, theoretically and technically, it can be applied to the real environment.

Based on our experiment with sample IDS data attack, it shows that the SLA Mapping is able to prioritize

<table>
<thead>
<tr>
<th>No.</th>
<th>Critical</th>
<th>Urgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Risk</td>
<td>Activity</td>
</tr>
<tr>
<td>8</td>
<td>Cost</td>
<td>Reliability</td>
</tr>
</tbody>
</table>
incidents with regard to the impact of the most dangerous intrusion by considering the critical sectors even though the same intrusion occurred in some targets.

IV. CONCLUSION AND FUTURE WORK

Prioritizing response service level agreement on the national critical sectors is very important as a national defense firm. The proposed system design is a design based on an analysis of several related works' protection needs and national security. Even though the design experiment has not been entirely carried out, it is hoped that the proposed design could be an alternative in determining security monitoring priorities effectively and on target.

Further research is still required as an in-depth analysis of the specific method used, in term of the appropriate decision-making method to be implemented in the real security monitoring system.

V. REFERENCES


[10] Ariani and M. Salman, "Intrusion Response System based on Time Management Concept with the Critical IP Address as a


Achieving 5G Security through Open Standards

A. Cheang¹, X. Gong², and M. Yang³

¹Huawei, Dubai, UAE
²Huawei, Shenzhen, China
³Huawei, Manama, Bahrain

¹aloysius.cheang@huawei.com, ²gongxiaoxin@huawei.com,
³yang.ming@huawei.com

ARTICLE INFO

Article History
Received 04 Feb 2020
Received in revised form 10 Feb 2020
Accepted 08 Mar 2021

Keywords:
5G, Cybersecurity, Privacy, Standards, NESAS

ABSTRACT

In telecommunications, 5G is the fifth generation technology standard for broadband cellular networks. The substantial increase in speed, coupled with reduced latency that allows instant communication and ability to connect more devices at the same time are critical game changers when it comes to building a foundation infrastructure that will support future smart applications and solutions in any digital transformation projects that attempt to create new outcomes that will benefit people and businesses. However, how do we ensure that a deployment of 5G is secure? How can experts ensure that 5G security risks can be effectively managed in terms of security protocols and standards as well as security assurance mechanisms? How to continuously improve 5G security level from the perspectives of different stakeholders in order to address future? This white paper will describe industry initiatives, joint efforts of industry partners and our proposal on how to build an open and transparent framework under OIC-CERT that will define a common baseline for 5G security across OIC member states.

I. INTRODUCTION

5G is a digital revolution, not just a speed-boost. 5G and the broadband bandwidth that it brings about allows for the realization of a real-time cloud, and the creation of applications and solutions that will enable the development of the next digital economy, enabling the smart city of the future and bridging the social divide leveraging on digital transformation that mines data as the new oil.

However, before 5G can takes flight the industry needs to resolve the security challenges and opportunities brought by new services, architectures, and technologies [1], as well as higher user privacy and protection requirements. The industry
needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks. Globally, the 3rd Generation Partnership Project (3GPP) SA Working Group (SA3) is tasked to look into security and privacy security issues in 5G. 3GPP SA3 quickly becomes the world’s leader in defining 5G security standards. SA3 held seven meetings. 74 companies (including their subsidiaries) sent technical experts to attend the meetings [2], with the key objective of formulating 5G security standards. The 3GPP SA3 has comprehensively analyzed 5G threats and risks in 17 security areas [3]: Security architecture, authentication, security context and key management, radio access network (RAN) security, security within NG-UE, authorization, subscription privacy, network slicing security, relay security, network domain security, security visibility and configurability, credential provisioning, interworking and migration, small data, broadcast/multicast security, management security, and cryptographic algorithms.

However, on top of the 3GPP security standards endorsement, operators need to develop a consistent end-to-end security framework that addresses both their network equipment and their network management. It should encompass more than just an operator's backhaul and core networks and base stations. Other network elements, such as interconnection gateways, firewalls, and IT servers (such as DHCP, DNS, and RADIUS servers) must also be considered in the overall security framework. By taking a holistic approach in designing such a framework, operators can ensure that there are no single points of failure within the network or at the border with other networks.

Besides operator’s overall design framework, there is also an imperative need to evaluate and benchmark the equipment such as mobile network equipment used in 5G deployment to meet the following requirement to achieve an impartial and high-quality standard in 5G deployment in any part of the world. This will be critical to ensure supply chain security though:

- Providing accreditation from the world's leading mobile industry representative body
- Delivering a world-class security review of security related processes
- Offering a uniform approach to security audits
- Avoiding fragmentation and potentially conflicting security assurance requirements in different markets

II. RELATED WORK

Several organisations have been working on designing architectures for telecommunication networks. Besides the heavily referenced 3GPP work in this paper, these are related work done by other projects such as:

- The NGMN (Next Generation Mobile Networks) Alliance’s 5G working programme [4], [5]. NFMN has identified new threats and security issues that may arise with 5G. In particular, the NGMN Alliance provides 5G security recommendations
for network slicing, access network, and low-latency use cases. For example, for network slicing, these recommendations express security needs of the infrastructure and virtualisation security realm.

- Resilient Communication Services Protecting End-user Applications from Disaster-based Failures or COST-RECORDIS [6], a European level consortium with scientific scope focusing on resilience of communication networks under disaster-induced failures. Such events can seriously disrupt a communication network, making its services unavailable. They follow from natural disasters, weather-induced disruptions, technology-related failures, or malicious attacks, and they are observably increasing in number, intensity and scale. When network services that are part of a critical infrastructure become unavailable, commercial and/or societal problems are the inevitable result. This COST Action, driven by researchers from academia and industry in strong cooperation with governmental bodies, aims to fill the gap by developing appropriate solutions to provide resilient communications in the presence of disaster-based disruptions of all types for existing and future communication network architectures.

- ETSI TC CYBER working group is recognized as a major trusted centre of expertise offering market-driven cyber security standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. ETSI TC CYBER [7] works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. They provide standards that are applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques. Specifically, on 5G security and 5G applications, these are their key research questions:
  - Mobile/Wireless systems (5G, TETRA, DECT, RRS, RFID...)
  - IoT and Machine-to-Machine (M2M)
  - Network Functions Virtualisation
  - Intelligent Transport Systems, Maritime
  - Broadcasting
  - Securing Artificial Intelligence
  - Privacy-preserving pandemic protection

III. METHODOLOGY

The following approach is adopted in our research methodology that is based on qualitative analysis methodologies, mainly Action Research [8] supported by Case Study and Narrative Models [9].
Action Research, or Participatory Action Research, is a reflective process of progressive problem solving led by individuals working with others in teams or as part of a "community of practice" to improve the way they address issues and solve problems. Whereas the narrative model occurs over extended periods of time and compiles information as it happens. Like a story narrative, it takes subjects at a starting point and reviews situations as obstacles or opportunities occur, although the final narrative does not always remain in chronological order. Businesses use the narrative method to define buyer personas and use them to identify innovations that appeal to a target market. Lastly, the case study model provides an in-depth look at one test subject. The subject can be a person or family, business or organization, or a town or city. Data is collected from various sources and compiled using the details to create a bigger conclusion. Businesses often use case studies when marketing to new clients to show how their business solutions solve a problem for the subject.

Thus, our research is performed according to the following time-based schedule:

A. Systematic literature review

To arrive at a key research focal direction based on the following research questions:

Question 1: What is the current 5G security controls in terms of baseline control sets and advanced control sets? How are they being developed into cyber security hygiene requirements?

Question 2: What are the efforts in establishing a common baseline for 5G security vis-à-vis various regulatory requirements and supporting deep tech applications?

Question 3: What is the work currently to engage all the stakeholders in the 5G ecosystem and how can that be improved?

B. Identify gaps or areas for performing Action Research

Arriving from an analysis based on literature survey, to build a systemic approach to ensure that a common baseline of key 5G security controls can be developed that will be adopted globally while reduce the gap (barriers of entry) and cost (reduce cost of entry) and harmonising regulatory requirement while matching technical capabilities.

C. Design Case Study / Reference Use Cases

As per required by Cast Study model, to develop use cases and reference models that can provide reassurance of the proposed solution framework effectiveness.

D. Continuous review of other 5G security research initiatives and progress

At the same time, to continue to scan the environment and review work done by other groups to ensure that any major security issues that are brought up can be addressed by this research
framework or that the risks can be mitigated by existing security controls proposed.

IV. KEY FEATURES OF 5G SECURITY STANDARDS

3GPP 5G security and 4G security share the same purpose, which is to ensure the confidentiality, integrity, and availability of networks and data. 5G Security Architecture inherits 4G Security Architecture, however provides Security Enhancement of 5G Standards over 4G Standards:

- Stronger air interface security: In addition to user data encryption on 2G, 3G, and 4G networks, 5G standards provide user data integrity protection to prevent user data from being tampered with.

- Enhanced user privacy protection: In 2G, 3G, and 4G networks, users' permanent IDs (international mobile subscriber identities — IMSIs), are transmitted in plain text over the air interface. Attackers can exploit this vulnerability using IMSI catcher attacks to track users. In 5G networks, users' permanent IDs (in this case, SUPIs) are transmitted in ciphertext to defend against such attacks.

- Better roaming security: Operators usually need to set up connections via third-party operators. Attackers can forge legitimate core network nodes to initiate Signaling System 7 and other attacks by manipulating third-party operators' devices. 5G Service-Based Architecture (SBA) defines Security Edge Protection Proxy (SEPP) to implement E2E security protection for inter-operator signaling at the transport and application strata. This prevents third party operators' devices from tampering with sensitive data (e.g. key, user ID, and SMS) exchanged between core networks.

- Enhanced cryptographic algorithms: 5G R15 standards currently define security mechanisms such as 256-bit key transmission. Future 5G standards will support 256-bit cryptographic algorithms to ensure that such algorithms used on 5G networks are sufficiently resistant to attacks by quantum computers.

5G cyber security standards put more security features into standard to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle.

V. THE NEED TO ENSURE CONSISTENCY OF EFFECTIVE 5G SECURITY CONTROLS IN DEPLOYMENTS BY ANY OPERATOR

Governments can be part of these efforts in controlling risks to operate 5G services in line with country regulations. A recommended win-win strategy to address 5G security is to deliver a plan described as follows:
• Formulation of regulations and laws, involving cross-discussion with all public and private partners, to guarantee a consistent security framework. Governments should take a key role here to define the requirements of their respective countries in terms of security and encourage the development of new technologies with risk control mechanisms to address both their economic objectives and security needs. This can be achieved through collaboration with all stakeholders, based on a common goal to define world standards. Governments play a major role in providing incentives to deliver a positive economic output for their respective countries, in terms of both leveraging innovations (5G in the context of this report) and guaranteeing that regulations are available for defining key aspects such as the security agenda, security assurance mechanism, certification program, and policies.

• Operators should be the major responsible body for the operation of network infrastructure and implementation of risk management according to the country's security regulations and official standards bodies. In addition to this, governments can implement specific policies to obtain oversight on the security level of each network operating in the country.

Towards this end, the Network Equipment Security Assurance Scheme/Security Assurance Specifications (NESAS/SCAS), jointly defined by GSMA and 3GPP, establishes a framework to facilitate improvements in security levels across the mobile industry [10].

VI. BUILDING SECURITY THROUGH INDUSTRY COLLABORATION TO TACKLE REAL WORLD PROBLEMS AND FUTURE SECURITY CHALLENGES

To truly control risks in the 5G lifecycle, besides continuously enhancing security solutions through technological innovation, efforts need to be expended to bring all stakeholders, from end users, government regulator, operators, technology providers and standardization or cyber security professional bodies together to build an industry-led open and transparent ecosystem cooperation so as to ensure that there is a common baseline of security control set and supply chain security.

Specifically,

• Technology providers: Technology providers should contribute industry security standard work, comply with standards, and integrate security technologies to build secure equipment. Together with customers and other stakeholders, vendors should provide capability to support the operators to assure secure operation and cyber
resilience. Thus, the security of the technology provided should be able to meet stringent certification requirements that are 3rd party, meet government regulator’s procurement requirement and recognized by different jurisdiction where you only need to be certified once, but accepted and usable by many.

- Operators: Operators are responsible for the secure operations and cyber resilience of their own networks. 5G networks are private networks. The boundaries between different networks are clear. Operators should build their own security defences based on zero trust architecture. For internal threats, operators can manage, monitor, and audit all vendors and partners to make sure their network elements are secure. Hence, through a zero trust approach to prevent against supply chain attack, operators need to have a defence in depth strategy that will heavily rely on a supply chain that has a common security baseline that is referenceable and can be relied upon through ecosystem cooperation.

- Industry and government regulators: As an industry, we all need to work together on standards. This is our shared responsibility. In terms of technologies, we need to continuously contextualize 5G security risks (in slicing, Mobile Edge Computing (MEC), massive Machine-Type Communications (mMTC) and other scenarios) and enhance protocol-based security. In terms of security assurance, we need to standardize cyber security requirements and ensure that these standards are applicable to and verifiable for all vendors and operators both locally and globally as part of a global ecosystem.

- End users: The end users should define key requirements that will be taken into account during standards development. They should be able to provide valuable inputs on actual 5G deployments security requirements especially in 5G to business applications.

- Cyber security professional bodies: The Cyber security professional bodies provide a platform for the ecosystem to leverage, that all stakeholders can come together in an industry-led effort to lead 5G security deployment in the locality that the bodies have a presence in. In fact, such a body like the OIC-CERT can play an important role to harmonise and enjoy economies of scale when it comes to pushing standards and certifications that are required to build the trust in any 5G business model, whether it is 5G to Consumers or 5G to Business.
As such, to build a system that we can trust, we need aligned responsibilities, unified standards, and clear regulation.

VII. FUTURE WORK

Leading from the previous Section, we propose OIC-CERT to set up a working group to look into 5G security for OIC member states to form a global trusted ecosystem for 5G. The working group shall aim at achieving the following:

- Identifying 5G cyber security risks taking into account different perspectives from the stakeholders and maintaining a risk register.
- Developing recommendations for our members, a 5G cyber security framework that be a reference model for member states to develop their own National 5G cyber security standards.
- Developing recommendations for developing an OIC-level 5G cyber security framework that harmonise the requirements that allow for cross-recognition among OIC member states.
- Subsequently to explore kick-starting another working group to develop an ISAC (Information Sharing and Analysis Centre) capability for CERT response in the era of 5G and Cloud for OIC member states under OIC-CERT.

On the other hand, we shall constantly scan the environment for any new 5G security updates, for example updates from 3GPP and update the 5G risk register in the proposed working group. For instance, 3GPP release 16 was completed on July 3, 2020. Looking ahead, SA3 are working on some exciting studies in release 17 [11], such as:

- Enhanced security support for Non-Public Networks.
- Security aspects of Unmanned Aerial Systems (UAS)
- Security for enhanced support of Industrial IoT
- Security Enhancements for 5G Multicast-Broadcast Services
- Security Enhancement of Support of Edge Computing in 5GC
- Security impacts of Virtualisation
- Authentication enhancements in 5GS
- Enhancements to User Plane Integrity Protection
- Security enhancement against false base stations
- Mission Critical Services Security Enhancement

Final release 17 was due 2021 has been shifted to 2022 due to the Covid-19 pandemic impact.

VIII. CONCLUSION

As more and more OIC member states embraces digital transformation, assumptions that need to be addressed such as unlimited bandwidth and unlimited storage will be the key addressable issues that
enable the realization of the vision to build a trusted digital oasis that will elevate the entire industry to the next level. 5G will provide that broadband connectivity that will address the need to provide unlimited bandwidth to bring us into Industrial 4.0 and support any Smart City, Smart Nation vision and it will be imperative that a common security baseline is defined for adoption of 5G such that minimum efforts are required for ensuring that any 5G deployment by any vendor or operator will meet the minimum security requirement for 5G regardless of which OIC member state or industry vertical that the 5G deployment is addressing where the outcome can be managed and measured with consistency without extensive time, effort and cost to go into assessing and certifying from scratch. This can be achieved through industry collaboration between different stakeholders in an industry-led open and transparent ecosystem cooperation that will build a secured and trusted supply chain for provisioning of broadband and any applications and solutions sitting on top of the broadband.

IX. REFERENCES


[10] Network Equipment Security Assurance Scheme [Online]. ISSN 2636-9680 etISSN 2682-9266

New Vulnerabilities upon Grain v0 Boolean Function through Fault Injection Analysis

Wan Zariman Omar@Othman\textsuperscript{1,2}, Muhammad Rezal Kamel Ariffin\textsuperscript{2}, Suhairi Mohd. Jawi\textsuperscript{1}, and Zahari Mahad\textsuperscript{2}
\textsuperscript{1}CyberSecurity Malaysia, Cyberjaya, Malaysia
\textsuperscript{2}Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia (UPM) Serdang, Malaysia
wanzariman@cybersecurity.my

ARTICLE INFO

<table>
<thead>
<tr>
<th>Article History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received 16 May 2020</td>
</tr>
<tr>
<td>Received in revised</td>
</tr>
<tr>
<td>form 26 Mar 2021</td>
</tr>
<tr>
<td>Accepted 30 Mar 2021</td>
</tr>
</tbody>
</table>

Keywords:
Vulnerabilities; Boolean function; Fault Injection Analysis (FIA); Stream Cipher; Annihilator

ABSTRACT

Algebraic attacks on stream cipher are very important in cryptography as well as in cryptanalysis. Generally, increasing degree of the equation will make an algebraic attack to the equation hardest. In conducting this analysis, we aim to decrease the degree of the targeted Boolean equation by constructing low degree annihilator equation(s). We adopt the Fault Injection Analysis (FIA) methodology to achieve our objectives. In this study, we found annihilator(s) through FIA (inject with value of one (1)) on Boolean function of selected stream ciphers. With the new injected Boolean functions developed, we proceed to utilize Hao’s method to find new annihilator(s). Then we established new annihilator(s) of Grain v0’s Boolean function. As a result, these newly identified annihilator(s) successfully reduce the complexity of the published Boolean function to guess the initial secret key. It also provides much needed information on the security and vulnerability of these selected stream cipher with respect to FIA.

I. INTRODUCTION

The objective of security is to protect against those who may harm intentionally or unintentionally. Security can be seen in many organizations, but this research prioritizes communication and information security. Communication security protects technology, media, and content. Meanwhile, information security protects the confidentiality, integrity, and availability. To ensure our information is secure, cryptology is one aspect to consider. As we all know, cryptology is a science that has two part:

1) Cryptography.
2) Cryptanalysis.

Cryptography originated came the Greek words that \textit{kripto} and \textit{graphia} which means \textit{hidden} and \textit{writing}. This technology of securing...
messages began since early civilization when human started to communicate and the need to keep their communication secret. The fundamental and classical task of this science is to provide confidentiality by encryption methods where both the encryption and decryption process used a secret key that was initially agreed by both parties. [1]

Cryptography has two types: asymmetric cryptography and symmetric cryptography. For symmetric cryptography, only one key will be used to encrypt and decrypt the data. Meanwhile for asymmetric cryptography, two different keys will be used to encrypt and decrypt. Asymmetric cryptography is also known as public key cryptography, it uses a pair of keys known as public and private keys to encrypt and decrypt data:
1) Public key: a key that can be shared with everyone and it is the key pair of the private key.
2) Private key: a key that must be kept secret by the owner.

For secret information transmission and storage, usage and implementation of symmetric key is very important. Both parties, the sender and receiver, share the same secret key. The sender and the receiver share the same secret key. To obtain the ciphertext, the sender must encrypt the message (plaintext) with a cipher and key. Ciphertext is usually transmitted over an insecure channel. The recipient must decode the ciphertext to get the original message with the same secret key. An attacker may decrypt the ciphertext, so a strong algorithm and strong key is highly recommended and should be used for encryption to ensure that the attacker does not have any information leaked. Rueppel points out the variations as in [2].

1) Block cipher: Operate with a fixed transformation on large block of plain text data.
2) Stream cipher: Operate with a time-varying transformation on individual plain text digits.

A. ATTACKS IN CRYPTOGRAPHY

In building a cryptosystem, a developer usually mathematician/cryptologist will build his or her best cryptographic algorithm meanwhile a cryptanalyst (also mathematician) will take opportunity to tackle the method of breaking the cryptosystem. All single analysis of and attack on each cryptosystem is very important because it will used to be a criterion to strengthen that particular cryptosystem. By [3], attackers in cryptography can be divided into two types:

1) Passive attacker
2) Active attacker and there are six (6) types of active attacks:
a) Chosen-plaintext attack
b) Chosen-ciphertext attack
c) Ciphertext only attack
d) Known plaintext attack
e) Adaptive chosen-plaintext attack
f) Adaptive chosen-ciphertext attack
B. TYPES OF STREAM CIPHERS

ATTACKS

Before we do an attack on or analysis of any stream cipher algorithms, it is very important to learn and understand all the possible attacks in stream cipher and the main purpose is to recover or discovering the key used in the process of encryption and decryption. By [4], there are ten (10) types of attacks in stream ciphers and each attack has their own method to recover or discovering the keys that were used. So from all ten (10) attacks, we are more focusing in Algebraic Attack and Fault Attack.

C. BOOLEAN FUNCTIONS IN

STREAM CIPHER

This subsection provides introduction to Boolean functions [5].

Definition 1. (Boolean function).
A Boolean function on $n$ may be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$.
A Boolean function $f(x_1,\ldots,x_n)$ is also can be written as the output of its truth table $f$.

Definition 2. (Algebraic normal form of Boolean function - ANF).
Every Boolean function $f$ can be expressed as a multivariate polynomial over $\mathbb{F}_2$. This polynomial is known as algebraic normal form of the Boolean function $f$.

Eq. 1 below showed the definition about Algebraic normal form of Boolean function.

\begin{equation}
\label{eq:ANF}
f(x_1,\ldots,x_n) = \sum_{\mathclap{\ell \leq n}} a_\ell \prod_{\mathclap{1 \leq i \leq n}} x_i^{b_{\ell,i}}
\end{equation}

D. ANNIHILATOR

As we mention in Definition 4, we let $g \in B^n$ an annihilator of $f$ function if $f \cdot g = 0$ or all $x \in \{0,1\}^n$. By [6], the existence of low-degree equations can be divided into three scenarios:

1) Scenario S3a: Assume that there exists a function $g$ of low degree such that the product function is of low degree, as example $f \cdot g = h$, where $h$ is a non-zero function of low degree.
2) Scenario S3b: Assume there exists a function $g$ of low degree such that $f \cdot g = 0$.
3) Scenario S3c: Assume there exists a function $g$ of high degree such that $f \cdot g = h$ where $h$ is non-zero and low degree.

But in 2004, [7] has reduced and improved method to find existence of low-degree equation to only one scenario. But via [8], we can effectively calculate...
all low-degree annihilators of both \( f \) and \( 1 + f \). Therefore, we choose this method together with FIA to obtain annihilator(s).

II. RELATED WORK

This paper focused on the cryptanalysis of stream cipher algorithm via their Boolean function. From previous work as [8] [9], there was few work or cryptanalysis on Grain family. So, from all this previous work, we narrow the research scope using fault injection attack as we refer to [11], [12], [13], [14] and [15].

III. METHODOLOGY

This section explains the research design used for conducting this research. The first step is collecting and understanding previous works. Secondly in Step 2, we will define each default general Boolean function of each selected stream cipher including identifying how many monomials (n) degree d of Boolean function.

A. Boolean Function

Given Boolean function

\[
h(x) = x_1 + x_4 + x_0x_3 + x_3x_4 + \]
\[x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + \]
\[x_1x_2x_4 + x_2x_3x_4 \quad (1)\]

where \( n = 5 \) variables and \( d = 3 \) (degree of Boolean function);

B. Fault Injection

This subsection explains how to inject fault value on Boolean function and generate a set of injected Boolean function. In this paper, we will inject (replace) value of one (1) to each active coefficient in each Boolean function. Replace each active coefficient of Boolean function \( h(x) \), starting with \( x_0 + x_1 + \ldots, + x_2x_3x_4 = 1; \)

Let Boolean function \( h(x) = x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4. \)

We define the following notation from Boolean function \( f(x_0, x_1, x_2 \ldots, x_k) \), the term \( B_{i_1, i_2, \ldots, i_j} \) refers to fault injection upon \( x_{i_1}, x_{i_2}, \ldots, x_{i_j} \). That is \( x_{i_1} = x_{i_2} = \ldots = x_{i_j} = 1 \). As an example:

\[
\begin{align*}
&\text{let } x_0 = 1 \implies B_0 = x_1 + x_4 + x_0x_3 + x_3x_4 + x_1x_2 + x_2x_3 + x_2x_4 + x_1x_2x_4 + x_2x_3x_4, \\
&\text{let } x_1 = 1 \implies B_1 = 1 + x_4 + x_0x_3 + x_3x_4 + x_0x_2 + x_0x_2x_3 + x_0x_2x_4 + x_2x_4 + x_2x_3x_4, \\
&\vdots \\
&\text{let } x_0 = x_1 = 1 \implies B_{0,1} = x_1 + x_2 + x_4 + x_0x_3 + x_3x_4 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4, \\
&\vdots \\
&\text{let } x_2 = x_3 = x_4 = 1 \implies B_{2,3,4} = 1 + x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 \\
\end{align*}
\]

C. Hao’s Method

In 2007, Hao [13] introduced sufficient and necessary conditions of the existence of low degree multiplies for a given Boolean function \( f \) is analyzed and three algorithms to find annihilators, \( g \) of a Boolean function \( f \). We consider all the \( n \) variable non-zero monomials of degree \( \leq d \) denoted by:
\( A_d = 1, x_1, x_2, \ldots, x_r, x_1 x_2, x_1 x_3, \ldots, x_1 x_r x_2, x_1 x_r x_3, \ldots, x_1 x_r x_2 x_3, \ldots, x_1 x_r x_2 x_3 \ldots x_n \)

\( = p_1 p_2 \ldots p_r (r = \sum_{i=1}^{n} C_i) \)

**Theorem 1.** \( |C| < A_d \implies \) There exists at least one annihilator of \( f \) with degree \( \leq d \).

**Theorem 2.** There exists annihilator of \( f \) with degree \( d \) \( \iff \) \( \text{rank}(M_d(h)) < |A_d| \).

**Algorithm 1** [8]: Given a \( n \)-variable Boolean function \( f \), find all annihilators of \( f \) with degree \( \leq d \).

1) Step 1: Construct matrix \( M_d(f) \).
2) Step 2: Convert \( M_d(f) \) into row ladder matrix \( M_d(f)^* \) using Gaussian elimination.
3) Step 3: If there exist zero-rows in \( M_d(f)^* \), it certainly exists an annihilator \( g \) of \( f \) and obtain \( g \) by using the inverse procession of Step 2, or else, there is no annihilator of \( f \) with degree \( \leq d \).

**Remark 1.** Construction of the matrix need evaluate \( fp_i \) on all \( x \in \{0, 1\}^n \), and it need many computations. If Boolean function \( f \) is represented by a \( 2^n \) vector, we can abbreviate these computations.

**Theorem 3.** \( n \)-variable Boolean function \( h \equiv 0 \), coefficients of \( h \) are zeroes. [8].

**Theorem 4.** There exists annihilator of \( f \) with degree \( \leq d \), The rows of \( N_d(f) \) are linear dependent \( \iff \) \( \text{rank}(N_d(f)) < |A_d| \). [8]

**Algorithm 2** [8]: Given an \( n \)-variable Boolean function \( f \), find all annihilators of \( f \) with degree \( \leq d \).

1) Step 1: Construct matrix \( N_d(f) \)
2) Step 2: Convert \( N_d(f) \) into row ladder matrix \( N_d(f)^* \) using Gaussian elimination.
3) Step 3: If there exist zero-rows in \( N_d(f)^* \), it certainly exists an annihilator \( g \) of \( f \) and obtain \( g \) by using the inverse procession of Step 2, or else, there is no annihilator of \( f \) with degree \( \leq d \).

**Theorem 5.** Let \( f \) be any Boolean function in \( B_n \). Then there exists annihilator of \( f \) with degree \( \leq d \) if and only if there exists \( h \in B_n \) with degree \( \leq d \) such that the degree of \( (1 + f) \cdot h = g \leq d \). [8]

**Algorithm 3** [8]: Given an \( n \)-variable Boolean function \( f \), find all annihilators of \( f \) with degree \( \leq d \).

**Input:** \( n \)-variable Boolean function \( f \)

**Output:** Boolean function \( h \) and \( g \) with degree \( \leq d \) such that \( g = (1 + f) \cdot h \)

1) Step 1: Define
\[
\sum_{i=0}^{d} c_i \times \sum_{i=d+1}^{n} c_i
\]
2) Step 2: Convert \( U_d(f) \) into row ladder matrix \( U_d(f)^* \) using Gaussian elimination.
3) Step 3: If there exists zero-rows in \( U_d(f)^* \) it certainly exists \( h \in B \)
with degree \( \leq d \) such that the degree of \((1 + f) \cdot h = g \) less than \( d \) and we can obtain \( h \) and \( g \) using the inverse progression of Step 2, or else there is no annihilator of \( f \) with degree \( \leq d \).

This algorithm 3 can generate all annihilators (with degree \( \leq d \)) of both \( f \) and \((1 + f)\).

IV. DESCRIPTION OF GRAIN v0

Grain v0 stream cipher was developed by [14] and the design was targets hardware that only have a very limited memory, limited power consumption and limited gate count. This algorithm was established on only two shift registers and one non-linear filter function namely an LFSR, an NFSR and a filter function as shown in Fig. 1.

A. Design of Grain v0

The content of LFSR is denoted as \( s_i \), \( s_{i+1} \), \( s_{i+2} \), ..., \( s_{i+79} \) meanwhile content of NFSR denoted as \( b_i \), \( b_{i+1} \), \( b_{i+2} \), ..., \( b_{i+79} \). The LFSR, \( f(x) \) feedback polynomial is a primitive 80 degree polynomial and is defined as:

\[
f(x) = 1 + x^{18} + x^{29} + x^{42} + x^{57} + x^{67} + x^{80} \quad (3)
\]

and this the update function LFSR to remove any possible ambiguity:

\[
s_{i+80} = s_{i+62} + s_{i+51} + s_{i+38} + s_{i+13} + s_i \quad (4)
\]

The feedback polynomial of the NFSR, \( g(x) \), shall be described as:

\[
g(x) = 1 + x^{17} + x^{20} + x^{28} + x^{35} + x^{43} + x^{47} + x^{52} + x^{59} + x^{65} + x^{71} + x^{80} + x^{17}x^{20} + x^{43}x^{47} + x^{65}x^{71} + x^{80}x^{28}x^{35}
\]

\[
+ x^{47}x^{52}x^{59} + x^{17}x^{35}x^{52}x^{71} + x^{20}x^{28}x^{43}x^{47} + x^{17}x^{20}x^{59}x^{65} + x^{17}x^{20}x^{28}x^{35}x^{43} + x^{47}x^{52}x^{59}x^{65}x^{71} + x^{28}x^{35}x^{43}x^{47}x^{52}x^{59} \quad (5)
\]

and this is NFSR update feature to eliminate any ambiguities: (including bit \( s_i \) that masked with the input in below function)

\[
b_{i+80} = s_i + b_{i+63} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} + b_{i+21} + b_{i+15} + b_{i+9} + b_{i+63}b_{i+60} + b_{i+33}b_{i+37} + b_{i+15}b_{i+9} + b_{i+60}b_{i+52}b_{i+45} + b_{i+33}b_{i+28}b_{i+21} + b_{i+63}b_{i+45}b_{i+28}b_{i+9} + b_{i+60}b_{i+52}b_{i+37}b_{i+33} + b_{i+63}b_{i+60}b_{i+21}b_{i+15} + b_{i+63}b_{i+60}b_{i+52}b_{i+45}b_{i+37} + b_{i+33}b_{i+28}b_{i+21}b_{i+15}b_{i+9} + b_{i+52}b_{i+45}b_{i+37}b_{i+33}b_{i+28}b_{i+21} \quad (6)
\]

B. Grain v0 Boolean function

Grain v0 Boolean function is given by;

\[
h(x) = x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4 \quad (7)
\]

Let \( n = 5 \) and \( d = 3 \) in the Grain v0.
V. Fault Injection Analysis on Boolean Function of Grain v0

As mentioned in previous section, Grain v0’s Boolean function is in equation 7. We will inject value of one (1) as fault value into each of active coefficient. In Grain v0, we obtained nineteen (19) active coefficients.

Let new generated Injected Boolean function of Grain v0 is as below (refer subsection III-B):

Let $x_0 = 1$
$$x_1 + x_4 + x_3 + x_3x_4 + x_1x_2 + x_2x_3 + x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (8)

Let $x_1 = 1$
$$1 + x_4 + x_0x_2 + x_0x_3 + x_2x_4 + x_4 + x_0x_2x_3 + x_0x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (9)

Let $x_2 = 1$
$$x_1 + x_4 + x_0x_1 + x_0x_4 + x_1x_4$$  \hspace{1cm} (10)

Let $x_3 = 1$
$$x_0 + x_1 + x_0x_2 + x_2x_4 + x_0x_1x_2 + x_0x_2x_4 + x_1x_2x_4$$  \hspace{1cm} (11)

Let $x_4 = 1$
$$1 + x_1 + x_3 + x_0x_2 + x_0x_3 + x_1x_2 + x_2x_3 + x_0x_1x_2 + x_0x_2x_3$$  \hspace{1cm} (12)

Let $x_0x_1 = 1$
$$x_1 + x_2 + x_4 + x_0x_3 + x_3x_4 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (13)

Let $x_0x_2 = 1$
$$x_3 + x_0x_3 + x_3x_4 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (14)

Let $x_0x_3 = 1$
$$1 + x_1 + x_2 + x_4 + x_3x_4 + x_0x_1x_2 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (15)

Let $x_0x_4 = 1$
$$x_1 + x_2 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (16)

Let $x_1x_2 = 1$
$$x_0 + x_1 + x_0x_3 + x_3x_4 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4$$  \hspace{1cm} (17)

Let $x_1x_4 = 1$
$$x_1 + x_2 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (18)

Let $x_2x_3 = 1$
$$x_0 + x_1 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_4 + x_1x_2x_4$$  \hspace{1cm} (19)

Let $x_2x_4 = 1$
$$x_0 + x_3 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3$$  \hspace{1cm} (20)

Let $x_3x_4 = 1$
$$1 + x_1 + x_2 + x_4 + x_0x_3 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4$$  \hspace{1cm} (21)

Let $x_0x_1x_2 = 1$
$$1 + x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (22)

Let $x_0x_2x_3 = 1$
$$1 + x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (23)

Let $x_0x_2x_4 = 1$
$$1 + x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_1x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (24)

Let $x_1x_2x_4 = 1$
$$1 + x_1 + x_4 + x_0x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_2x_3x_4$$  \hspace{1cm} (25)
Let $x_2 x_3 x_4 = 1$

$$1 + x_1 + x_4 + x_0 x_3 + x_1 x_4 + x_0 x_1 x_2 + x_0 x_2 x_3 + x_0 x_2 x_4 + x_1 x_2 x_4$$

From the analysis via FIA and HAO’s algorithm on Grain v0, we achieved possibility of annihilator(s). Consequently, we can obtain that only six (6) active coefficients in Boolean injected function generated zero row in $Md^*$. The coefficients involved that generated with one (1) zero row in $Md^*$ is:

1) $x_0$
2) $x_1$
3) $x_2$
4) $x_3$

Meanwhile we get two (2) zero rows in $Md^*$ each for injected into coefficients, $x_3$. We also obtained four (4) zero rows in $Md^*$ by injected into coefficients $x_0 x_2$.

VI. ILLUSTRATION OF REDUCING BOOLEAN FUNCTION DEGREE VIA NEWLY FOUND ANNIHILATORS

For this section, we will illustrate our result on Grain v0 by using Theorem 5. We achieved six matrices, $Md^*$ that have zero row(s) when we injected the fault value via coefficients $x_0$, $x_1$, $x_2$, $x_3$, $x_4$ and $x_0 x_2$, but only injection Boolean function via $x_4$ produces annihilators.

For the case $x_1$, we achieved $f = 1 + x_4 + x_0 x_2 + x_0 x_3 + x_2 x_4 + x_3 x_4 + x_0 x_2 x_3 + x_2 x_3 x_4$. The corresponding annihilator $g = x_2 + x_1 x_4 + x_1 x_3 + x_2 x_4$. The degree of $h$ is 2 and is the same as $(1 + f)$.

For the case $x_2$, we achieved $f = x_1 + x_4 + x_0 x_3 + x_0 x_4 + x_1 x_4$. The corresponding annihilator $g = x_0 x_4 + x_2 x_4$ did not reduce the complexity to find the initial key string of the injected Boolean $f$; of the form $1 + f$. We observed $(1 + f) = g = h = x_0 x_2 (1 + x_1 + x_4 + x_1 x_4) + x_0 x_3 (1 + x_2 x_4)$. The degree of $h$ is 2 and is the same as $(1 + f)$.

For the case $x_2$, we achieved $f = x_1 + x_4 + x_0 x_3 + x_0 x_4 + x_1 x_4$. The corresponding annihilator $g = x_0 x_4 + x_2 x_4$ did not reduce the complexity to find the initial key string of the injected Boolean $f$; of the form $1 + f$. We observed $(1 + f) = g = h = x_0 x_4 (1 + x_1 + x_2 + x_1 x_2)$. The degree of $h$ is 2 and is the same as $(1 + f)$.

Next, when we injected the Grain v0 Boolean function via $x_4$, we obtained $f = x_0 x_1 x_2 + x_0 x_3 + x_1 x_2 + x_2 x_3 + x_0 x_1 x_2 + x_0 x_2 x_3$. The corresponding annihilator $g = x_0 x_1 + x_1 x_2$. Observe that $(1 + f) = g = h = (x_0 x_1) + (x_0 x_1 x_2) = x_0 x_1 (1 + x_2) = u_1 u_2$ where $u_1 = (x_0 x_1)$ and $u_2 = (1 + x_2)$.

For the case $(1 + f) = 1$, we assumed $u_1 = 1$ and $u_2 = 1$, and obtained Table I. It shows that in our case the complexity of guessing the initial key bit is $2^0 = 1$. This is a reduction from the complexity of $2^4 = 16$ upon the published Grain v0 Boolean function.

We obtained one first degree and one second degree simultaneous equation instead of third degree equation. If $(1 + f) = 1$, then we have few combinations of $u_1 u_2 = 1$. We assume that $u_1 = 1$ and $u_2 = 1$ and we generate Table I and managed to get only $2^0 = 1$ complexity of guessing compared with the published Boolean of Grain v0 that has $2^4 = 16$ complexity to guessing initial key bit.

<table>
<thead>
<tr>
<th>$x_0$</th>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$(1 + f)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

For the case $(1 + f) = 0$, we assumed either $u_1 = 1$ and $u_2 = 0$ or $u_1 = 0$ and $u_2 = 1$ or $u_1 = 0$ and $u_2 = 0$ and
obtained Table II. It shows that in our case the complexity of guessing initial key bit is 7. This is reduction from the complexity of $2^4 = 16$ upon the published Grain v0 Boolean function.

### Table II: Grain v0 Combination

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$(1 + f)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

### VII. DISCUSSION

From the analysis and results we have generated eighteen injected Boolean functions and successfully obtained three possible annihilator(s) from Grain v0's Boolean function via FIA with Hao’s method. We then identified that the annihilator, $g = x_0x_1 + x_1x_2$ which was obtained by injecting fault value upon $x_4$, had capacity to reduce the complexity of determining the initial key upon our injected Grain v0 Boolean function as showed in Table III. That is from complexity of $(24 = 16) + (24 = 16) = 32$ to $(20 = 1) + 7 = 8$. In conclusion this identified annihilator provided much needed information on the security of Grain v0 and will be utilized to launch algebraic attacks upon Grain v0 stream cipher.

### Table III: Annihilator upon Grain v0’s Injected Boolean Function

<table>
<thead>
<tr>
<th>Coefficient</th>
<th>Annihilator</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_4$</td>
<td>$x_0x_1 + x_1x_2$</td>
</tr>
</tbody>
</table>

### VIII. CONCLUSION

As for the conclusion, this paper successfully conducted a Fault Injection Analysis (FIA) on Boolean function of selected stream cipher such as Grain v0. For Grain v0 stream cipher, we got four coefficients that produced one zero row, one coefficient that produced two zero row and one coefficient that produced four zero row. But only three of this output generate possible annihilators as in Section VII; $x_2 + x_1x_2 + x_1x_3 + x_2x_4$, $x_0x_4 + x_2x_4$ and $x_0x_1 + x_1x_2$. So, from eighteen generated injected Boolean function, we only found three annihilators but only this annihilator $x_0x_1 + x_1x_2$ manage to reduce degree and complexity of published Boolean function.

### IX. FUTURE WORKS

We planned to do analysis for another algorithms that have more complicated Boolean function as Grain v1 or Grain-128 and Rakaposhi algorithms. Hopefully, we can manage to get funding to conduct future research.

### X. REFERENCES
