Counter-Narrative Cyber Security Model to Address the Issues of Cyber Terrorism

Ahmad Syafiq Ahmad Tamerin[1], Nur Azaliah Abu Bakar[2]*, Noor Hafizah Hassan[3], and Nurazean Maarop[4]

[1]*Malaysian Armed Forces, Inspectorate General Branch, Ministry of Defense, Kuala Lumpur, Malaysia*

[2]*Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur Malaysia*

syafiq_tamerin@yahoo.com; azaliah@utm.my; noorhafizah.kl@utm.my; nurazean.kl@utm.my

Article history

Received:
30 October 2019

Received in revised form:
15 November 2021

Accepted:
1 December 2021

Published online:
21 December 2021

*Corresponding author
azaliah @utm.my

Abstract

Terrorism is the imminent threat that Malaysia and the entire world are facing nowadays. This has become a severe threat to Malaysia's national security as extremist groups such as ISIS and DAESH are leveraging cyberspace to gain more supporters and sympathisers. These extremists used social media to disseminate their narratives among the Malaysian Armed Force (MAF) personnel to recruit them for their excellent military skills. Nevertheless, the current MAF counter-narrative is still using traditional media operations like roadshows, brochures dissemination, articles, and short videos in combating the terrorism agenda, which are less effective and time-consuming. Therefore, this study proposes an enhanced counter-terrorism approach to fight this terrorism narrative by utilising the MAF IT infrastructure to focus on the social media platform. The model was built based on ISO / IEC 27032:2012 standard, concerning three cyber-terrorism models. Six military IT experts then verified this new enhanced model. They agreed that it is crucial to establish such a model and emphasise that counter-terrorism effort needs full cooperation with other services and collegiality. This study's final output is the Counter-Narrative Information Technology Model, which will later potentially be adopted to the MAF environment in line with the national inspiration in fighting terrorism.

Keywords: *counter-narrative; cybersecurity; Malaysian Armed Forces; militant; military*

1. Introduction

Today, the entire world is faced with the threat posed by foreign terrorist organisations. The focus is on the risks of terrorism activities by the group known as DAESH (ad-Dawlah al-Islāmiyah fīl-ʿIrāq wash-Shām) and established in June 2014 by Abu Bakar Al Baghdadi in Iraq. This group today actively worked under the aim of promoting some form of the political structure in the Khilafah Islamiyah (the Muslim government), planning to establish or grow a Khalifah (a ruler who leads the people of the world), the system of government in the Khilafah Islamiyah (the Islamic government) and the state or country that a political and religious leader (like the Khilafa Salis) governs.

Until the end of 2018, DAESH had accomplished worldwide, other than Iraq and Syria, with 143 attacks in 29 countries, killing 2,043 and injuring a thousand more [1]. In Malaysia, there have been 389 people arrested in connection with DAESH and sharia-like rebels who have been fighting against the Malaysian government.

* *Corresponding author.azaliah@utm.my*

They claimed that the number of militant supporters increased based on the growing number of people arrested due to this movement. [2]. A proof of their attack can be seen in the explosion at the Movida Night Club, Kuala Lumpur, in 2016; fortunately, no fatalities were reported. [3].

As highlighted by [4], terrorist nowadays not only are they attacking in real life, but they are also moving beyond cyberspace. With the advancement of information technology and digital platform, the DAESH group has leveraged social media, especially Facebook, to threaten the Malaysian with a series of bombing, weapon attacks, and kidnapping attempts [5]. Social media is used to connect and share information among the ISIS militants and foreign terrorists throughout this region with their leaders in Syria. According to Datuk Ayob Khan, Royal Malaysian Police (RMP) Special Branch Counter-Terrorism Division Head, 95 per cent of new DAESH recruitments in Malaysia was based on social media, especially Facebook [6]. It is revealed that more than 3,800 Facebook accounts are treated as militants and terrorism in Malaysia. In 2014 and 2015, 11 Malaysian Armed Forces (MAF) members were held after being radicalised by terrorist groups and other extremist ideologies. A few of these people were believed to acquire weapons for the attack of the Malaysian government. [7].

The United Nations (UN) has developed a counter-terrorism policy called the "United Nations Counter-Terrorism Strategies, "strongly supported by the Malaysian government. The strategies consist of four pillars that prevent, protect, pursue, and respond, as shown in Figure 1.

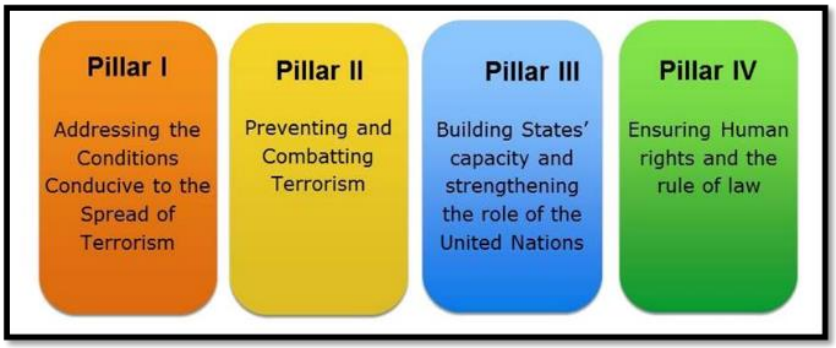

Figure 1: United Nations Counter-Terrorism Strategies

In Malaysia, RMP has collaborated with Counter Messaging Centre (CMC), MAF, to detect and hinder the DAESH narrative and propaganda spreading. As a way of keeping an eye on MAF personnel, the Cyber Defence Operation Center (CDOC) had been building up their cyber team to track MAF's contact with the militant group, such as the DAESH; in fighting them from spreading the DAESH ideology within the MAF personnel (CDOC) [8].

The MAF CDOC was set up to assist the MAF Intelligence Department and Digital Strategic Communications Division (DSCD) in countering terrorism. The CDOC launched the Task Force Perisai Wira initiative intending to establish the Counter Violent Extremism (CVE) and counter-narrative strategies which is consist of five primary activities which is 1) the identification of terrorism narratives, 2) the

creation of counter-narrative content, 3) the selection of forum, 4) the dissemination and 5) the monitoring [8].

CVE aims to prevent individuals or groups from recruiting new followers, supporters, facilities, or engagement with terrorism activities. The idea of CVE is to engage and communicate with these peoples, group them into the micro-level, and make these groups move to the right of the community and enact a more pragmatic stance on political, religious, or social issues. [9]. While, the concept of counter-narrative is to fight against extremist recruitment and propaganda, thus discerning the terrorist ideologies and violent extremists [10]. Therefore a strategic communication is required with a different approach. It is suggested that alliances be formed between MAF agencies or departments for expanded contact and data collection, reaching out to the target audiences.

Nevertheless, the Task Force Perisai Wira CVE and counter-narrative are still based on a conventional approach to disseminating counter-narrative messages, such as face-to-face contact and roadshows pamphlets dissemination, articles publishing, and posters exhibition [11]. This is strongly supported by [8] that stated these modern media age methods are obsolete and less successful than the terrorist narrative that these extreme groups are broadcasting. The Perisai Wira Task Force initiative needs to be digitised to understand this critical void immediately. This effort should be made between agencies to deliver counter-narrative messages with robustness.

This study focuses on Pillar I and Pillar II of United Nations Counter-Terrorism Strategies, which implements the soft approach in combating the terrorist group. Figure 1 shows the United Nations Counter-Terrorism Strategies. Therefore, this study focuses on the soft approach in combating terrorism in a MAF environment that consists of CVE and counter-narrative on digital platforms concentrating on social media. This study aims to develop a new MAF model to control and monitor the influence of terrorism narrative among MAF personnel on social media and digital platforms. This will assist the MAF in counter-violence extremism and significantly become the new military cybersecurity baseline in fighting terrorism in this country.

2. Related Studies

Terrorism originates from the Latin word “Terrere,” which means to generate nervousness and anxiety. According to Hoffman and Morrison-Taw [12], Terrorist means acts of violence, and Terrorism means creating tensions and fear, thereby attracting the attention of the peoples’ communities. In the meantime, cyber terrorism is described as the use of cyber technologies for enabling, disruptive. Destructive cyberspace militant operations to build and exploit fear through violence or the threat of violence in pursuit of political change [13].

On the contrary, [14] mention that counter-terrorism is also known as anti-terrorism, focusing on a rigid approach that cooperates with tactics, strategies, and strategies involving government, military, law enforcement, business, and intelligence agencies to combat or prevent terrorism. CVE employs non-coercive steps to discourage individuals or organisations and reduce non-state recruitment,

promotion, facilitation, or involvement in politically motivated terror to pursue political objectives. [9]. CVE aims to prevent individuals or organisations from attracting new followers, supporters, services, or participation in terrorist activities. One of the techniques in CVE is counter-narrative, which is countering radical recruiting and propaganda by suppressing terrorist agendas and violent extremists' actions.

2.1 New Terrorism Phenomenon

The phenomenon of terrorism has become more complex, and it sparked a new dimension of the threat to international security. The recent dimension of terrorism is called "new terrorism," which witness how the advancement of technology leads the terrorist media centre to spread their narrative and ideology in cyberspace and reach more potential recruits through the social media platform [13, 14]

According to Harun [8], there are five most common narratives disseminate by DAESH through their media platform either in the cyber forum or traditional media formats such as magazine, newspaper, and pamphlets, which are Narrative 1 – Jihad has become an individual obligation (fardhu ain), and Jihad has no meaning other than qital (war); Narrative 2 –Emigration (hijra) is a must for Muslims who want to reach the perfection of faith and uplift life in an Islamic State; Narrative 3 – DAESH is promoting a comfortable life and Musli brotherhood under the rule of their Caliphate; Narrative 4 – DAESH is promoting Syria and Iraq as a perfect ground to perform Jihad; and Narrative 5 – The DAESH Caliphate is the 'true land of Islam' and emigration (hijra) to it is ordered and compulsory

2.2 Countering Terrorist Narratives

Counter-terrorism refers to the action taken in fighting the threats of terrorism act either in real life or the digital world. Previous researchers' review reveals several types of countering terrorist narrative, consisting of government strategic communication, alternative narrative, and counter-narrative [10, 12]. According to the Radicalisation Awareness Network (RAN), counter-narrative can be divided into type involves key characteristics and stakeholders should take care of the action [15]. Table 1 describes the counter-terrorism narrative in detail.

Table 1: Types of Counter-Narrative

What	Why	How	Who
Government Strategic Communications	Action to get the message out about what the government is doing, including public awareness activities	Raise awareness, forge relationships with key constituencies and audiences, and correct misinformation	Government
Alternative Narratives	Undercut violent extremist narratives by focusing on the organisation 'for' rather than 'against.'	A positive story about social values, tolerance, openness, freedom, and democracy	Civil society or government
Counter Narratives	Directly deconstruct, discredit and demystify violent extremist messaging	Challenge through ideology, logic, fact, or humour	Civil society

Through the Southeast Asia Regional Centre on Counter-Terrorism (SEARCCT), the Malaysian government conducted a counter-terrorism narrative to set up a "mental firewall" for the target audience, especially the young generation, to counter radical ideologies are exposed to. Hundreds of digital counter and narrative products, including digital banners, videos, and digital comics on major social

media platforms, were designed and produced by SEARCCT. Furthermore, [5] showed that Malaysia has also established efforts with other partner countries in this region through the MAF Digital Strategic Communications Division (DSCD) to utilise the soft approach in countering terrorism on the internet, mitigating radicalisation and recruitment in the ASEAN region. In MAF, the Task Force Perisai Wira team was responsible for studying, researching, and delivering the counter-messaging, including intelligently gathering the data from the ground and cyberspace to create a strong counter-narrative message MAF personnel. They had produced articles, banners, posters, videos, and roadshows at MAF camp and entire base Malaysia to avoid the MAF personnel getting involved with DAESH.

The legislation is the one action of countering terrorism, and the Malaysian government had produce and extensive legislation according to the current terrorism situation and threats [8]. Several laws are used to prohibit the Malaysians from engaging in terrorist acts and radical action, consisting of:

1) Internal Security Act 1960 (Act 82) repeal in September 2011.
2) Penal Code.
3) Security Offences (Special Measures) Act (SOSMA) 2012 (Act 747).
4) Prevention of Crime (Amendment and Extension) Act (POCA) 2014.
5) Prevention of Terrorism Act (POTA) 2015.
6) Special Measures against Terrorism in Foreign Countries Act (SMATA) 2015.
7) Anti-Money Laundering Act (AMLA) 2003.
8) Special Measures against Terrorism in Foreign Countries Act (SMATA) 2015.

However, the MAF environment is different from a typical Malaysian environment. They are linked and bound with the Armed Forces Act 1972 and inclusive with the other civil laws. MAF personnel is strongly prohibited from joining an illegal organisation such as DAESH, JI, or KMM as indicate in the Unit or Formation Standing Operational Procedures (SOP), MAF General Command, Services General Order, Public Service Provider (PSD) Regulations 1993 and the Public Service Disciplinary Regulations 1993 (Harun, 2016). Any MAF personnel cannot participate in such activities or retain any information relating to a terrorist group such as:

1) CDs that promote DAESH activities.
2) Videos that promote DAESH terrorism or that encourage migration to Islamic State
3) Brochures/articles (soft and hard copy) promote DAESH’s activities or the Caliphate they are fighting for.
4) Video games from the production of Al Hayat Media Center.
5) 'Hijrah to Islamic State'.
6) DABIQ Magazine (soft and hard copy).
7) T-Shirt, sticker, emblem, flag, or ISIS logo that promotes this group.

8) Any magazine/leaflet or newsletter associated with DAESH is produced by any country or any other organisation in the world that promotes the cause, activity, or Islamic Caliphate of DAESH

2.3 Comparison of Current Counter-Narrative Framework

In fighting the DAESH narrative, much organisation has come out with its counter-terrorism framework. The three most comprehensive counter-narrative frameworks are from Hedayah Center: the International Center of CVE located in Abu Dhabi, U.A.E. (https://www.hedayahcenter.org), the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) (https://www.searcct.gov.my), and the MAF counter-narrative model by Task Force Perisai Wira Unit. This study analysed the existing frameworks based on nine distinctive elements: process, agencies, platform, target audiences, collaborations, legislation, evaluation, objective, and detention. Table 2 shows the comparison of these three frameworks used in counter-terrorism efforts against these militant or extremist groups.

Table 2: Comparison of three counter-narrative frameworks

No.	Element	Hedayah Center	SEARCCT	MAF
1.	Process	Ended process	Ended process	Circulating
2.	Agencies	Government	Government	MAF Elements
3.	Platform	Inter-Agencies	Inter-Agencies	MAF Assets
4.	Target Audiences	Citizen of the country	Malaysian	MAF Personnel
5.	Collaborations	Integration with agencies involved	Integration with agencies involved	Inter-department in MAF
6.	Legislation	All related laws to the terrorism and crime act	All related laws to the terrorism and crime act	Additional, with Armed Forces Act 1972
7.	Evaluation	Focus on the counter-narrative and messages	Focus on the counter-narrative and messages online	Questionnaires and validation form
8.	Objective	Difference between agencies	Difference between agencies	Similar objectives
9.	Detention	Local authorities to detain suspect influenced to terrorism narrative	Local authorities to detain suspect influenced to terrorism narrative	Collaboration with local authorities

From the analysis, it can be concluded that the Hedayah Center and SEARCCT counter-narrative framework are designed as an ended process focused on the citizen as a whole. They also support the inter-agencies platform and are based on the terrorism/crime act. However, the Task Force Perisai Wira is different, whereby their target audiences, legislation, and objectives concentrate on MAF's military aspect.

2.4 Implementing the ISO/IEC 27032:2012 Cyber Security Guideline for MAF Counter-Terrorism

In recent years, no doubt that cybersecurity is crucial in protecting critical infrastructures, including the government, utility, and military resources and assets [16]. The ISO/IEC 27032:2012 Information Technology – Security Techniques – Guideline for Cybersecurity is the international standard that can provide a guideline focusing on technical aspects and management. It consists of several domains covering information security, network security, internet security, and critical information infrastructure protection (ISO, 2012). The ISO/IEC

27032;2012 approach for defining cybersecurity is classified into communication security, operation security, information security, physical security, and public, national, and military security. Figure 2 shows the Logical relationships between cybersecurity and other security domains.

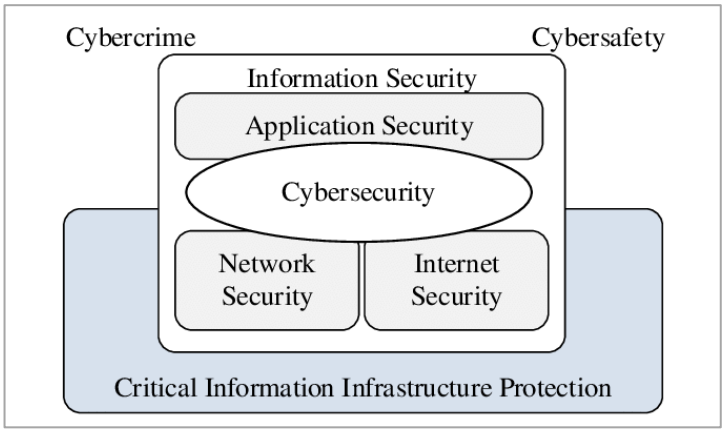

Figure 2: Logical relationships between cybersecurity and other domains [17]

The ISO/IEC 27032 standards provide the guideline that consists of 1) Stakeholders in the cyberspace; 2) Assets in the Cyberspace; 3) Threats against the security of the cyberspace; 4) Roles of stakeholders in cybersecurity; 5) Guidelines for stakeholders; 6) Cybersecurity controls, and 7) Framework of information sharing and coordination. Due to its comprehensiveness, it can comply with any form of the organisation, either for business, government sectors, or military aspects [18]. Building on the concepts and framework specified in ISO/IEC 27001, the best practice guidance and techniques outlined in ISO/IEC 27032 can help MAF prepare for, detect, monitor, and respond to cyber-attacks.

3. Methodology

This study focuses on counter-violence extremism (CVE) and counter-narrative activities through MAF's information technology platform. The aim is to identify all the CVE and counter-narrative activities and design a suitable counter-narrative IT model for MAF. This study's IT platform's scope is the official social media, official website portal, and mobile application on the smartphone. This study methodology has four phases: 1) Investigation, 2) Development, and 3) Evaluation. The following are a detailed explanation.

3.1 Investigation Phase

This phase starts with problem identification, gathered from academic journals, articles, and other related newspapers or agencies reports on the terrorism and counter-terrorism atmosphere in Malaysia and the region. The current guideline and framework in counter-narrative will support this research and adopted to the MAF environment situation.

3.2 Development Phase

The development phase focused on designing the model based on combining the previous study and existing frameworks from other researchers. This study chooses

four frameworks as the baseline: the ISO 27032:2012 Information Technology – Security Technique – Guideline, the Hedayah Center guideline, the SEARCCT guideline, and the MAF Counter-Terrorism guideline itself since the focus is within the MAF environment. A comparative analysis was conducted to analyse the security elements and related activities from each framework.

3.3 Evaluation Phase

This evaluation phase consists of two activities, which are data collection and data analysis. The purpose is to investigate the terrorism phenomenon in MAF and confirm if the literature's proposed elements also match the condition of the terrorism threat in MAF. The study approach is qualitative. The data collection is based on an interview with MAF Subject Matter Experts (SME). The respondents were from Cyber Defence Operation Centre (CDOC), Intelligence Department, and Digital Strategic Communications Division (DSCD) in MAF Kuala Lumpur. This research's sampling is based on purposive sampling that focuses on expert sampling [19]. The participants' profile comprises military intelligence, such as counter-terrorism, media operation, and cybersecurity. The participants also were selected based on their academic level with at least a bachelor's degree and had more than seven years of experience in this area. The list of participants is shown in Table 4.

Table 4: List of Participants in this Study

Name	Background	Area of Expertise	Designation	Experience (years)
A1	Army	Terrorism	Head of Task Force Perisai Wira	More than 20 years
A2	Air Force	Intelligence and Strategic Study	Head of Air Force Intelligence Department	More than 20 years
A3	Ex-Army	Intelligence and Psychological Operation	SME of Psychological Operation Department	More than 30 years
A4	Army	Media Operation	Head Armed Forces Head Quarters Strategic Communication	More than 20 years
A5	Navy	Media Operation	Staff Officer of Navy Head Quarters Strategic Communication	More than nine years
A6	Army	Cyber Security	Staff Officer Cyber Defence Operation Centre (Awareness)	More than nine years

Series of interviews were conducted with the selected MAF senior officer and counter-terrorism SME's in MAF. The data collected from the interviewees are interpreted into the enhancement of the proposed model from the analysis of the existing counter-narrative frameworks. The model is shown to the interviewees to analyse and review before giving their opinions and comments. The interviews' result was analysed based on the thematic analysis technique [20]. This technique is chosen because of its flexibility to any particular epistemological and theoretical perspectives. This technique aims to identify the themes and patterns of the data collection related to this research. The following are the steps in conducting the thematic analysis.

1) Select and group within similarities expertise
2) Select the same pattern as the grouping.
3) Exploit all the data and merge it within it.
4) Modify d the model based on the data analysed.

The final analysis result was used to enhance the proposed model as suggested by the experts

4. Proposed New Counter-Narrative IT Model for MAF

The proposed model consists of five primary activities representing the daily operation of the CVE counter-narrative in MAF CDOC, ranging from identification, analysis, production, dissemination, and monitoring. The identification, analysis, and monitoring are considered the 1st Phase Counter-Narrative. All these activities are under the counter-terrorism department, which is the task Force Perisai Wira Unit. The counter-narrative production and dissemination activities will be under each respective department's responsibility. They know the best way to convey those counter-narrative messages within their team. Figure 3 shows the new counter-narrative proposed model for MAF.

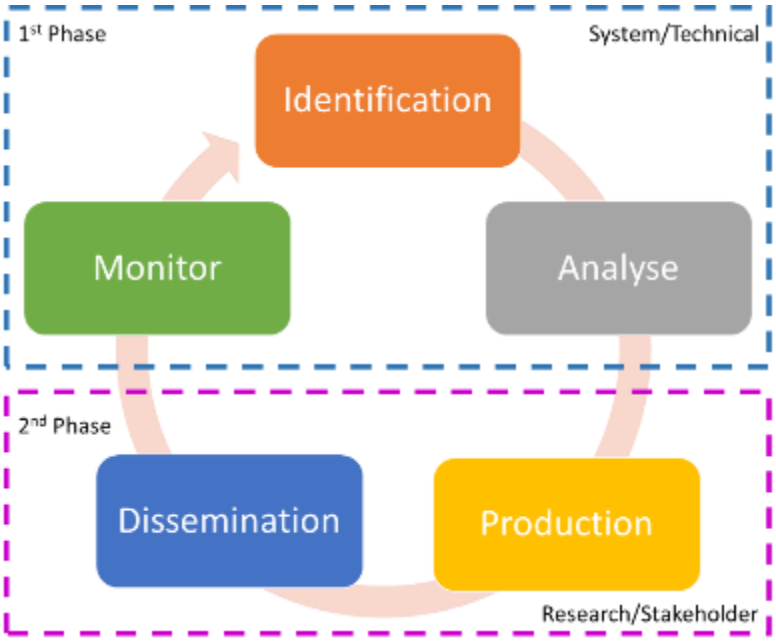

Figure 3: New counter-narrative IT model for MAF

To strengthen the existing counter-narrative framework in the cybersecurity aspect, this study benchmarked those frameworks to ISO/IEC 27032:2012, as shown in Table 3.

Table 3: Analysis of the existing counter-narrative frameworks

Security Element	Activities	ISO 27032:2012	Hedayah Center	SEARCCT	MAF	Total
Stakeholders roles in collaboration	Security collaboration between agencies	✓	✓	✓	-	3
	Effort between Services	-	✓	✓	✓	3
Exposure and Threats Management	Spreading/hacking of malware by Terrorist	✓	✓	-	-	2
	Spreading of terrorist narratives	✓	✓	✓	✓	4
	Awareness: Online	✓	✓	✓	-	3

Security Element	Activities	ISO 27032:2012	Hedayah Center	SEARCCT	MAF	Total
	Awareness: Offline	-	-	-	✓	2
Risk assessment and treatment	Reporting the detection/incident handling	✓	✓	✓	✓	4
Guidelines	Control of terrorist training and recruitment of new followers	-	✓	-	✓	3
	CVE and Digital/Online Counter-Narrative Enforcement	-	✓	✓	-	4
Cybersecurity controls	Digital Platform: Social Media, Online Communication Apps	✓	✓	✓	-	3
	Dissemination Approach: Terrorist Narrative/Propaganda Video, Images (Poster), Article	-	✓	✓	✓	4
A framework of information sharing and coordination	Dissemination of the counter-narrative message	-	✓	✓	✓	4
	Platform usage	✓	✓	✓	-	3
	Media operation	✓	✓	✓	✓	4
	Exchange information bilateral/multilateral	✓	✓	✓	✓	4
	TOTAL	**9**	**14**	**12**	**10**	-

From the analysis, this study found out that the MAF framework lacks clear roles of stakeholders CVE and counter-narrative digital security collaboration between agencies. Besides, it also scarce of asset protection on the control over hacking or spreading the malware by the Terrorist, which leads to threat exposure through an online platform. It is also missing the guidelines on CVE and digital/online counter-narrative enforcement, and finally, the framework does not include the cybersecurity control on social media, online communication apps, and digital platform

Besides, the MAF environment is not the same as other government agencies or countries because the military officers are subjected to Armed Forces Act 1972, which means they can be on court-martial if they do not follow the order to leave any involvement in terrorist activities. In terms of inter-agency collaboration, MAF only will do so when given the authority orders. Nevertheless, all frameworks focus on a hard approach, which can easily be observed by the series of people detained due to terrorist activities compared to a soft system that has hardly been discussed on its success and effectiveness. Realising this gap, we aim to incorporate the IT standards and compliance with the existing MAF CVE and counter-narrative strategy to support the soft counter-terrorism approach by enhancing the digital platform and cybersecurity aspects.

5. Model Evaluation Results

The following section explains the interview findings' details according to security elements and activities evaluated, as discussed in the previous section. Table 5 shows a summary of the items.

Table 5: List of Security Elements and Activities Evaluated

Security Element	Activities
Stakeholders roles in collaboration	Security collaboration between agencies
	Effort between Services
Exposure and Threats Management	Spreading/hacking of malware by Terrorist
	Spreading of terrorist narratives
	Awareness: Online
	Awareness: Offline
Risk assessment and treatment	Reporting the detection/incident handling
Guidelines	Control of terrorist training and recruitment of new followers
	CVE and Digital/Online Counter-Narrative Enforcement
Cybersecurity controls	Digital Platform: Social Media, Online Communication Apps
	Dissemination Approach: Terrorist Narrative/Propaganda Video, Images (Poster), Article
The framework of information sharing and coordination	Dissemination of the counter-narrative message
	Platform usage
	Media operation
	Exchange information bilateral/multilateral

5.1 Stakeholders Roles in Collaboration

All interviewees mentioned that they would keep communicating with Task Force Perisai Wira to share the current intelligence and information on terrorist activities. They will support Task Force and ensure that the MAF is always ahead in combating terrorist and militant activities in the Malaysian and MAF environments.

[…] The report keeps updating the cybersecurity threats to the whole process so that everybody is aware of the threats. Later the awareness program can be synchronised with the counter-narrative materials by Task Force Perisai Wira if needed. […]-Interviewee A7.

Collaboration is a must in a vast organisation with three MAF branches: the Malaysian Army, Royal Malaysian Navy, and the Royal Malaysian Air Force. Without collaboration and cooperation between them, the top echelon's solid decision-making is challenging to achieve. It may affect the subordinates on the ground. Counter-terrorism, counter-violence extremism (CVE), and counter-narrative need directives from the top management. Thus, action and planning must be done with a collaborative spirit. Each service will conduct the same agenda in fighting terrorism between their subordinates. The previous studies by Stephens and Sieckelinck [21] and Sumpter [22] identified that one of the obstacles to CVE initiatives' success is the lack of strong support from relevant state agencies in forming an effective collaboration. Therefore, in this new proposed model, security roles in collaboration are critical components to be included.

All interviewees agree that the MAF stakeholders give their support and commitment to fighting terrorism to their subordinates. Intelligence Department plays a vital role in leading other services in conducting CVE and counter-narrative; simultaneously, the Intelligence Department and DSCD collaborate with other government agencies to identify any MAF personnel associate with any terrorist groups. According to Interviewee A3, the cooperation between all agencies is crucial, especially in intelligence and information sharing of any terrorism issue, because uncontrolled early terrorism activity will affect Malaysia's safety and security.

[…] Intelligence Department always communicates with MAF reps for intelligence and information, either terrorism environment or other security proposes. This collaboration keeps us always update on the current situation, either in real life or cyber. The intelligence and information then will be submitted to the selected department to take on for terrorism activities and submit to Task Force Perisai Wira for following action […]-Interviewee A3.

For Task Force Perisai Wira, the collaboration with another counterpart internationally for intelligence and information sharing. The efforts are by conducting several forums or workshops between bilateral or trilateral partners. According to Interviewee A1, this requires a collaborative effort between various departments to ensure they will get a clear picture of the current environment of terrorism activities entire region that may affect Malaysia.

5.2 Exposure and Threat Management

This CVE and counter-narrative exposure and threat management are widely broadcast to the MAF personnel by directive and order from the higher echelons. However, they are not notified that the counter-narrative materials are one of the efforts. This is because the materials that are being broadcasted are mostly the just look alike Anti-Terrorism campaign.

The materials that consist of articles and e-posters exposed to MAF personnel on digital platforms are also printed and distributed by their departments and branches. According to interviewees, they are agreeing with the effort done by Task Force Perisai Wira in their campaign in delivering the counter-narrative materials from seminars or forums because, at the same time, the audiences know that what had been broadcast by the strategic communication department before this.

5.3 Risk Assessment and Treatment

The Task Force Perisai Wira play a vital role in gathering all the counter-narrative source. Currently, the CDOC and Counter-Intelligence Directorate (CID) departments share their information with Task Force Perisai Wira team from the cyber perspective. Meanwhile, the Operation and Strategic Directorate (OSD) shares the ground field or physical data source. The Task Force Perisai Wira team will then consolidate and disseminate those counter-narrative materials to every department in MAF.

According to all interviewees, they received the counter-narrative messages and material from Task Force Perisai Wira, either in digital or physical materials. Later, they used it for distribution within their media platform. Sometimes the material will be filtered before the distribution process due to the confidentiality level. As a consequence, this has delayed the counter-narratives information dissemination among the MAF personnel. Interviewee A2 also emphasised the consistency of the materials to be disseminated for the counter-narrative activity.

[…] Task Force Perisai Wira's centralised materials keep us updated on the same situation and messages for our subordinates because we work at the same place together. Suppose the messages or counter-narrative materials are the difference between Services or departments. In that case, we may have a different understanding […]-Interviewee A2.

5.4 Procedure and Guidelines

All interviewees agreed that the current procedure's achievements and impact show that only several people reach the counter-narrative materials posted on the official portal and social media such as Facebook and Twitter. The counter-narrative materials' impact is difficult to identify because the MAF did not survey the materials being posted. Instead, MAF focused on broadcasting good images on their platforms. The current practice is just one-off broadcasting upon the counter-narrative materials received from Task Force Perisai Wira.

As suggested by Carthy et al. [23], the counter-narrative exercise needs to be consistently executed, hence from long and consistent practice, it will become a strong culture in any organisation. Therefore a guideline must be established to control CVE and support the counter-narrative activities. At the same time, it also mitigates any terrorist soft approach for the recruitment of new followers among the MAF.

5.5 Cybersecurity Controls

MAF had produced a directive in controlling the use of social media for everybody. All the interviewees agree that MAF must keep the information posted over the official portal and social media. According to interviewees A3 and A7, CDOC and Counter-Intelligence Directorate monitor the online platform where CDOC monitors and eliminates any attack or penetration into the network that links with the official portal. Counter Intelligence Directorate monitors the social media of MAF personnel. It will report any suspicious MAF personnel with a sign of sympathy, support, or attraction to join the terrorist groups. In the meantime, cybersecurity awareness had been conducted from time to time to expose the MAF personnel to the cybersecurity threat. The awareness campaign is to keep MAF personnel from being a victim of cyber-crime and at the same time to avoid them from being manipulated by Terrorists as recruiters or sympathisers.

[…] Social engineering is an attack vector that tricks people into breaking routine security procedures. So we are working to ensure personnel that uses the official portal are not exposed to this attack and try to keep our network with higher security. We keep monitoring other attacks such as malware, phishing, and other threats that may harm our system and keep the attacker stole our data for any purposes […]-Interviewee A7

All interviewees agree that the current platform used is good enough to disseminate the counter-narrative materials. The platform consists of the official portal and social media such as Facebook, Twitter, telegram, WhatsApp, and YouTube. The official portal links up with the official organisation email. At the same time, the Webmaster can use this platform in disseminating the counter-narrative material. According to interviewee A5, organisation email is widely used to engage others that duty away from the organisation.

[…] Webmaster played an essential role in controlling the portal's materials and posted them after getting approval from the department's head. Sometimes navy.mil being used for a delivery directive that involves two ways of communication. RMN was implementing the Chief of Navy forum via Video Conference weekly to discuss among the senior officer from several headquarters around Malaysia. Sometimes, this forum is used to share the current situation of counter-terrorism. […]-Interviewee A5

According to interviewee A1, the traditional platform had approved a good achievement in delivering the counter-narrative messages and through the survey. However, today there is a need to use the online platform because the target audiences are young people, university students, secondary school students, and teenagers. There is a need to use the media to exploit the counter-narrative materials through the digital storyteller, e-posters, short cartoon-like Abdullah X Series recognised by the UK Government, series of digital comics, and other funny or catchy slogans that may keep the target audiences to avoid from involving the terrorism activities.

Interviewees said that all the digital counter-narrative materials had been posted on the official portal and social media platform. The official platforms control by the StratComm department and post the base of the material on the current issues where the materials came from Task Force Perisai Wira while they are maintaining the traditional media platform to deliver their narrative messages. According to Interviewee A1 and A2, communication is the best platform because anybody who needs clarification can get the information directly from the subject matter expert.

[…] We (Task Force Perisai Wira team) went down to the ground to meet the people and deliver our narratives to keep the people's get the proper knowledge about DAESH. At the same time, we want them to leave any activities that may involve them in DAESH, which may lead them to accuse any law link to terrorism. We use traditional media, and at the same time, we give the digital copy to any StratComm department to broadcast/post on their official and social media platform. […]-Interview A1.

[…] Two communication from top to bottom and bottom-up by face to face is the best way. However, an IT platform is relevant because it is fast and easy to deliver messages or narratives. The platform's use helps a lot in disseminating the message. Sometimes we call upon Task Force Perisai Wira to provide in forum or seminar to our staff […] -Interview A2.

5.6 The Framework of Information Sharing and Coordination

This model can be the best exchange for counter-narrative materials' content to be shared with other departments. This element is added in the model supported by all interviewees because everybody can update the terrorism activities in the MAF and national environment.

[…] Every counter-narrative material that had been produced should consist of a theme, symbol, messages (based on the objectives), and the spoke person (if available or needed). The material should pre-test the acceptance (available for digital or traditional media); modification is necessary when the pre-test is required if no improvement proceeds for approval. I agree with the mode; you should combine the target audience, spoke persons, and platform as one element that can refer to the triangle hierarchy. Add some features such as National Law, National Security Council Orders No.18 and directives from the MAF in the guideline bases. The Stake Holder should involve the Ministry of Defence to answer to the government as well. […] -Interviewee A3.

6. Discussions

The evaluation results from the experts showed some improvement over the proposed model methods. The new modified model will only covered the production and dissemination process, which is the second phase of the counter-narrative approach. Meanwhile, this model's first phase focuses on the system and technical operation to identify, analyse, and monitor proposes. This phase involves an expert in cybersecurity to detect and identify the terrorist attack or terrorist use of the internet targeting MAF personnel.

As suggested by the experts from the interview session, these three processes will be under the respective department's responsibility and not part of the Counter-Narrative Cyber Security Model governed by MAF CDOC. In this new Counter-Narrative Cyber Security Model, the second phase focuses on the counter-narrative materials cycle, starting from production until the dissemination process.

In the production process, the focus is on the counter-narrative messages' production, whereby the risk assessment and threat management activities will be conducted. This is also has been used in another similar study by [24]. A counter-narrative message is designed based on the assessment result, including the terrorism narratives and cybersecurity threats. Together with the report is the proposed cybersecurity controls as a guide. The same report and counter-narrative messages consisting of policy, strategic, and broad messages will be distributed from the top, middle, operation, and tactical levels.

The dissemination platform includes the leading mass media, services official portal, and official social media platform. As for the tactical group, the counter-narrative messages need to be more specific for the army's aim on the fields. This is based on earlier research, which shows that people are engaged in structured communities and connected to social networks and active in recognisable subcultures [25]. The explanation is that social ties influence recruiting activists, a longing for glory, and disappointment with their homeland's lives than by ideological factors [26, 27]. Furthermore, a study by [28] has proven that any sentiment analysis can be easily detected if the organisation leverages this vast growth of social media such as Twitter and Facebook as their early detection of cyber threats. Hence, this model emphasises publishing any suitable counter-narrative publicly on social media because it can influence and invite future collaboration with other agencies to give online awareness and digital platform sharing. Figure 4 shows the detailed model of the MAF Counter-Narrative Cyber Security Model.

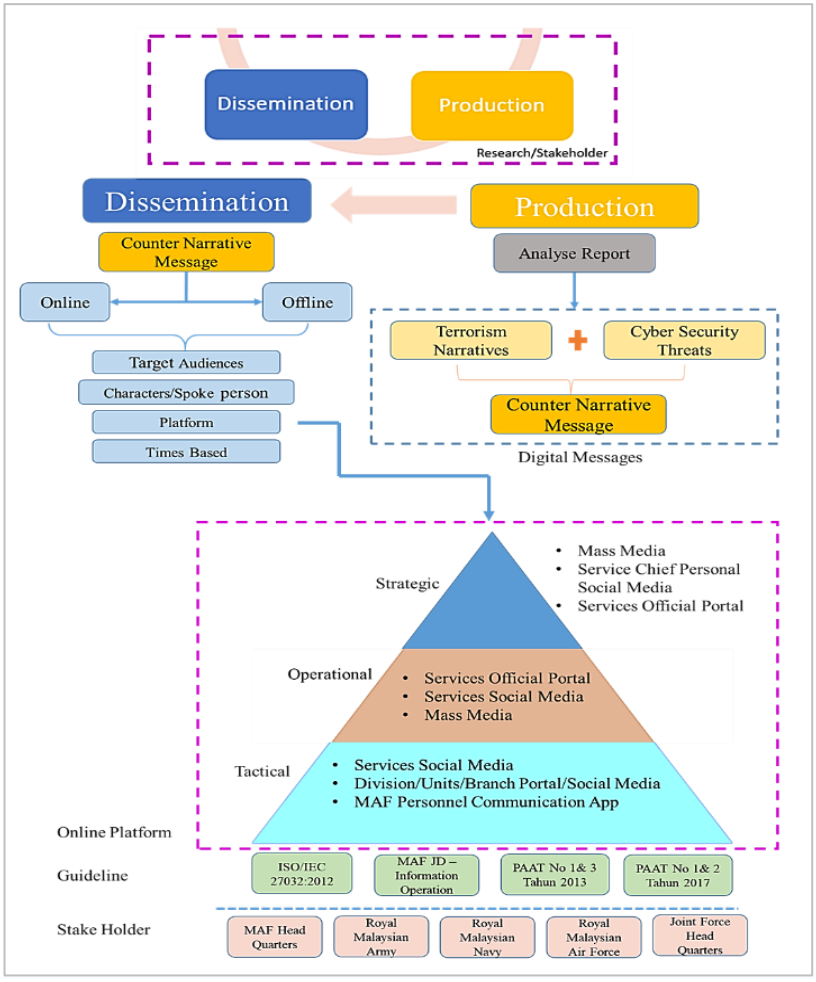

Figure 4: MAF Counter-Narrative Cyber Security Model

As discussed in the findings section, stakeholders play an essential role in collaboration. The stakeholders are the main focus in achieving the target and ensuring all the MAF personnel received the messages. They are the primary role in ensuring all the counter-narrative materials to design and produce with deterrence withstanding with the nation's desire. The second layer includes the guidelines, including the previous three counter-narrative frameworks and ISO/IEC 27032:2012 standard discussed earlier. The triangle shows the hierarchy of the platform and how the counter-terrorism messages should be disseminating. With these two main processes, we can demonstrate that MAF is successfully embedded in the counter-narrative model's cybersecurity elements, aiming for information sharing and coordination between agencies.

7. Conclusions

Overall this work offers an enhanced approach to combat the terrorism agenda by introducing Counter-Narrative Cyber Security Model. This study's strength is that we can show how MAF could improve counter-terrorism by utilising IT operations and cyberspace with ISO/IEC 27032:2012 standard as a guideline. This will resolve the issues highlighted earlier on the missing cyberspace counter-terrorism action in the existing MAF initiative. This study's results have been

embodied in a practical application whereby it consolidates both cybersecurity threat awareness and CVE narrative messages, facilitating MAF in informing the cyber terrorism threat to the armed forces. In practicality, the model can be utilised by Task Force Perisai Wira and MAF Strategic Communication Department in their daily operation. Instead of promoting the MAF, this model shall be one of their SOP one day if this model is recognised and approved by the MAF at the higher echelon. If possible, this model can bring up to the doctrine development level because MAF working instruction and operation are based on the doctrine either by single service or joint-ness process.

Nonetheless, the study has its limitations, especially regarding the study scope, which only focuses on Task Force Perisai Wira and the small number of experts evaluating the model. For future work, this research can be used for upgrading the traditional media operation into cyber or internet bases media operations. The model's scope can also be extended to the whole counter-narrative process proposed earlier, namely, identifying, analysing, and monitoring, which is not addressed in the final results. Furthermore, the model can be refined by investigating the latest technology infrastructure required to support this model design, mainly when the terrorist group, like the DAESH, is always ahead in acquiring new technology. Nevertheless, this model provides further evidence that future work relies on MAF cooperation with other government agencies, counterparts, and the new order from the Malaysian government in fighting terrorism activities in Malaysia.

Acknowledgments

Thanks to the MAF personnel, the research team generously shared their time, experience, and materials for this study. The Author(s) declare(s) that there is no conflict of interest in producing this research article.

References

[1] S. Schulman, "No Exit: Outside the Camp, Daesh Incidents are on the Rise. Inside, Tempers are Seething," *The RUSI Journal*, vol. 164, no. 7, pp. 54-67, 2019.

[2] M. I. Abd Razak, R. A. A. Rahim, M. A. Ramli, M. Y. Yusof, P. H. Salleh, and N. I. Kasmaruddin, "Religious Extremism & its Recruitment Methods: An Analysis," *Journal of Administrative Science*, vol. 16, no. 1, pp. 34-50, 2019.

[3] H. Wahari, "Pihak Berkuasa Malaysia Sahkan IS Dalangi Kes Letupan Kelab Malam," in *Bernama News Channel*, ed. Kuala Lumpur: Bernama, 2016.

[4] S. Macdonald, D. Grinnell, A. Kinzel, and N. Lorenzo-Dus, "Daesh, Twitter and the Social Media Ecosystem: A Study of Outlinks Contained in Tweets Mentioning Rumiyah," *The RUSI Journal*, vol. 164, no. 4, pp. 60-72, 2019.

[5] W. F. A. W. Zakaria, "Ancaman Ideologi Keganasan: Faktor-Faktor Penglibatan Masyarakat Malaysia dalam Kumpulan Daesh: Ideology of Terrorism's Threat: The Factors of Malaysian Community that Involved in DAESH," *'Abqari Journal,* pp. 111-127, 2020.

[6] N. Hussin and N. I. Nasri, "95 Peratus Pengganas Daesh Direkrut Menerusi Media Sosial.," in *Utusan Malaysia Online*, ed, 2018.

[7] T. C. Anuar and M. Hadzman, "Militan IS rancang beli senjata serang Malaysia," in *Utusan online*, ed: Utusan, 2015.

[8] Z. Harun, "Melawan Naratif-naratif IS/ISIS/DAESH," in "Berita Tentera Darat Malaysia," Markas Tentera Darat, Wisma Pertahanan, Kuala Lumpur2016, Available: https://army.mod.gov.my/phocadownload/buletin/206.pdf, Accessed on: 1 Feb 2020.

[9] B. Baruch, T. Ling, R. Warnes, and J. Hofman, "Evaluation in an emerging field: Developing a measurement framework for the field of counter-violent-extremism," *Evaluation*, vol. 24, no. 4, pp. 475-495, 2018.

[10] A. Reed, H. J. Ingram, and J. Whittaker, "Counter-narratives, Alternative Narratives, and Government. In Countering Terrorist Narratives," Brussels2017, Available:

https://www.europarl.europa.eu/RegData/etudes/STUD/2017/596829/IPOL_STU(2017)596829_EN.pdf .
[11] J. Jawhar, "Terrorists' Use Of The Internet: The Case Of Daesh," *Kuala Lumpur, Malaysia: The Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs*, 2016.
[12] B. Hoffman and J. Morrison-Taw, "A strategic framework for countering terrorism," in *European democracies against terrorism*: Routledge, 2019, pp. 3-29.
[13] M. D. Putra, "New Media and Terrorism: Role of the Social Media to Countering Cyber Terrorism and Cyber Extremism for Effective Response," *Available at SSRN 2754370*, 2016.
[14] A. J. Raj, "10 Challenges in counter-terrorism and counter violent extremism in Malaysia," *Countering Insurgencies and Violent Extremism in South and South East Asia*, 2019.
[15] C. Mattsson, N. Hammarén, and Y. Odenbring, "Youth 'at risk': A critical discourse analysis of the European Commission's Radicalisation Awareness Network Collection of approaches and practices used in education," *Power and education*, vol. 8, no. 3, pp. 251-265, 2016.
[16] L. A. Maglaras *et al.*, "Cybersecurity of critical infrastructures," *ICT Express*, vol. 4, no. 1, pp. 42-45, 2018.
[17] *ISO/IEC 27032: 2012–Information technology—Security techniques—Guidelines for cybersecurity*, 2012.
[18] B. von Solms and R. von Solms, "Cybersecurity and information security–what goes where?," *Information & Computer Security*, 2018.
[19] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approach*. Sage publications, 2017.
[20] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77-101, 2006.
[21] W. Stephens and S. Sieckelinck, "Working Across Boundaries in Preventing Violent Extremism: Towards a typology for collaborative arrangements in PVE policy," *Journal for Deradicalization*, no. 20, pp. 272-313, 2019.
[22] C. Sumpter, "Countering violent extremism in Indonesia: priorities, practice and the role of civil society," *Journal for Deradicalization*, no. 11, pp. 112-147, 2017.
[23] S. L. Carthy, C. B. Doody, K. Cox, D. O'Hora, and K. M. Sarma, "Counter-narratives for the prevention of violent radicalisation: A systematic review of targeted interventions," *Campbell Systematic Reviews*, vol. 16, no. 3, p. e1106, 2020.
[24] A. AlMajali, K. M. A. Yousef, B. J. Mohd, W. Dweik, S. A. Ghalyon, and R. a. Hasan, "Semi-quantitative security risk assessment of robotic systems," *Jordanian Journal of Computers and Information Technology (JJCIT)*, vol. 4, no. 03, 2018.
[25] T. Bjørgo, "Processes of disengagement from violent groups of the extreme right," in *Leaving terrorism behind*: Routledge, 2008, pp. 48-66.
[26] S. Atran, *Talking to the Enemy: Faith, brotherhood, and the (un) making of terrorists*. Harper Collins, 2010.
[27] D. Duriesmith and N. H. Ismail, "Embodied militarism and the process of disengagement from foreign fighter networks," *Critical Military Studies*, pp. 1-17, 2019.
[28] S. Kumar, V. Koolwal, and K. K. Mohbey, "Sentiment analysis of electronic product tweets using big data framework," *Jordanian Journal of Computers and Information Technology (JJCIT)*, vol. 5, no. 1, pp. 43-59, 2019.