Fusion or Fantasy

Is Cyber Fusion Living Up to the Dream?

Anne Coull
Flinders University
Sydney, Australia
email: anne.coull@proton.me

Abstract— The Cyber Fusion Centre has evolved from a military and antiterrorist intelligence gathering centre to become an intelligence focus for collating information and facilitating cyber incident management in organisations. Some benefit is being realised in Australia's larger banks as they manage the challenge of coordinating cyber response across disparate and siloed teams. These simple Cyber Fusion Centres provide basic, manual, reactive coordination of cyber incidents by generating open communication between response teams. This basic fusion model being implemented in Australian banks, and documented in the FS-ISAC whitepaper, is miles from the visionary Cyber Fusion Centre models described in the literature. These theoretical centres of response excellence incorporating strategic threat intelligence, orchestration, crisis simulations and ultimate real-time response-capability are well beyond the current reality. The answers for closing the gap between theory and practice can be found by looking into the original military fusion centres.

Keywords- Cyber Fusion Centre; Intelligence; Counterinsurgence Operations; Counterterrorism; Crisis Management.

I. INTRODUCTION

As the coordination centre for cyber intelligence and response within an organisation, the Cyber Fusion Centre would appear to be the logical place from whence to drive accelerated response to cyber security incidents. The literature describes the Cyber Fusion Centre as a collaboration between threat intelligence, incident response, threat hunting, and vulnerability management, with the purpose of accelerating identification and response to security threats. A fusion centre of this nature will enable an organisation to accelerate response by removing delays through orchestrating cyber response activities that span multiple departments and teams. By sharing strategic intelligence, it will allow the organization to be more proactive in their cyber response, pre-emptively preparing for and mitigating the emerging threats, rather than just responding to threats after the alerts have been generated, and the incidents have occurred.

The Cyber Fusion Centre emerging in Australian banks, and documented in a whitepaper by the Financial Services Information Sharing and Analysis Center (FS-ISAC), is a simple model of collaboration between security, service management, and customer service. The fusion centre team's role is to coordinate response activities involving these and other operations and technical support teams. This model is based on Cyber Fusion Centre capabilities operating in banks and organisations in the United States, Canada, Singapore, and Australia. Utilising fusion in this way reduces potential threat impact by decreasing time to identify complex and critical incidents and time to respond, but it does not deliver the scale of uplift nor the benefits anticipated in the literature.

Section 2 outlines the evolution of fusion centres from military coordination centres to intelligent Cyber Fusion Centres. Section 3 assesses the cyber fusion theory versus the reality. Section 4 looks at how Cyber Fusion Centres have been implemented in Australia and delves into a specific instance in a large Australian bank to highlight opportunities for improvement, and Section 5 provides insight into how the gap between the theory and reality can be closed.

II. CYBER FUSION EVOLUTION

Fusion centres have functioned as operations' response coordination centres since mankind participated in multi-domain warfare. Over time, the fusion centre model has evolved into a centre for intelligence, co-ordination, and information sharing, in response to terrorist incidents and the growth of cyber-crime.

A. Military Fusion Centres

For decades, fusion centres have operated in the military as Joint Operations Centres, to co-ordinate operations across the multiple domains of war: land, sea, air, and space, and more recently cyberspace [1][7][11][13][14] (see Figure 1).

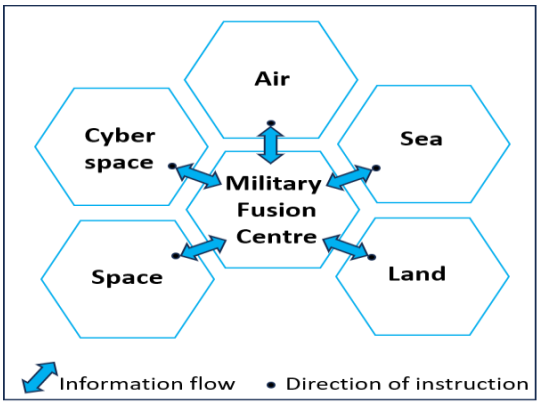

Figure 1. Military Fusion Centre.

 ISBN: 978-1-68558-113-8

Military fusion has enabled more efficient and effective offensive and defensive operations by providing broad situational awareness and facilitating coordination of activities across different regions, regiments, and domains.

B. *Counterinsurgency Operations' Intelligence Fusion and Flow*

Counterinsurgency operations (COINOPS) take this need for intelligence fusion and flow to a high level. To stay abreast of enemy movements, COINOPS need tangible real-time intelligence. This sensitivity is driven by COINOPS role working closely with both military and civilian populations. Insurgencies involve mixtures of conflict and tactics across multiple domains, topographies, and offensives. Information flow is critical during counterinsurgency operations' when this information needs to be disseminated from/to headquarters (HQ) and the front-line troops and commanders in real-time. Rather than having all the intelligence capabilities centralised in military HQ, the key is to have technology and personnel, with the necessary capabilities, implanted through all layers of the intelligence information flow, from front line platoons and commanders to HQ. These may be specialised language translators and intelligence analysts, or military personnel holding these skills [11] (See Figure 2).

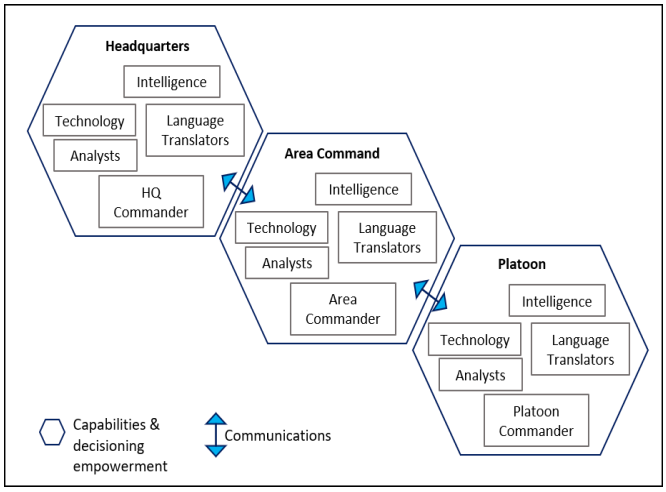

Figure 2. COINOPS Model.

C. *Counterterrorism Intelligence Fusion Centres*

Following the New York twin tower attacks on September 11, 2001, in the U.S., fusion centres evolved from wartime and operational co-ordination centres into centres for collating and correlating terrorist intelligence. In the U.S., the Department of Homeland Security (DHS) was created at the national level, to bring together intelligence and law enforcement. Correspondingly, law enforcement, public security, and emergency response were also centralised at the state level. Fusion centres were created to connect the local and state intelligence centres with federal intelligence organisations and services. This amalgamated model facilitates the flow of counterterrorism (CT) intelligence from/to local to/from federal [15] (See Figure 3). The purpose of creating a combined model of intelligence, law enforcement and emergency response was to drive more efficient and effective offensive and defensive intelligence-enabled security, public safety, and emergency response, through communications, collaboration, and coordination across these different capabilities at the state and national levels [15].

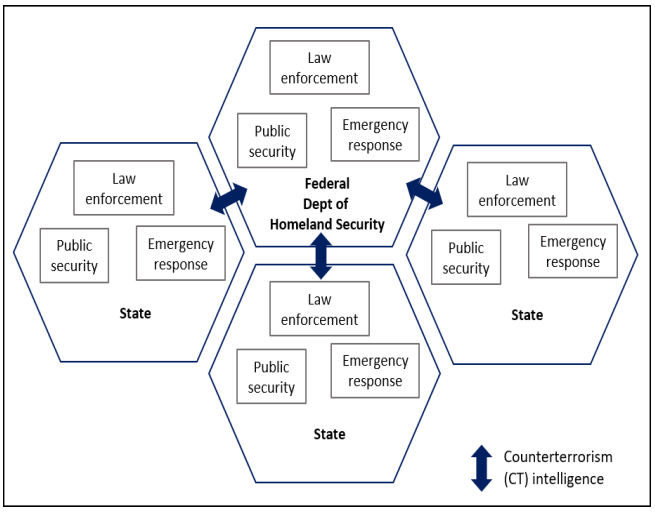

Figure 3. DHS Fusion Centres [15].

D. *Intelligent Cyber Fusion Centres*

As security leaders moved from roles in military defence into business, they saw the need, in their new organisations, for Intelligent Cyber Fusion Centres to drive more efficient and effective intelligence-enabled cyber response and incident management, through integrated intelligence and operations. As a result, Cyber Fusion Centres have been established in a number of larger organisations across the United States of America, and in some of the larger Australian Banks.

A Cyber Fusion Centre (CFC) is described in the literature as a physical or virtual entity created through collaboration between threat intelligence, incident response, threat hunting and vulnerability management, with the purpose of identifying, managing, and rapidly responding to security threats. This may be a separate team, a virtual team with representation from the local response teams, or a blend, with a small group of individuals facilitating and coordinating aggregation, collation, and distribution of information across the participating teams, and analysing this integrated information to identify themes and correlations [1][3][4][15][16]. The theoretical Cyber Fusion Centre accelerates threat response by bringing together:

1. Technical Threat Intelligence such as attack vectors, suspicious domains, malware hashes, and exploited vulnerabilities to assess the cyber threats facing the organization;

 ISBN: 978-1-68558-113-8

2. Strategic Threat Intelligence to map attack trends, motivations, and characteristics;
3. Analysis of this intelligence to generate insights about threats and adversary behaviours, Tactics, Techniques and Procedures (TTPs), and Indicators Of Compromise (IOC) [1]-[3].
4. Cyber incident management [6].

As it matures, the fusion centre will extend to deliver:

1. Security Orchestration, Automation and Response (SOAR), with automated operational workflows to facilitate incident triage, threat pattern analysis, and automated threat response capabilities;
2. Response plan testing and crisis simulations to prepare for major incidents; and
3. Short and long-term recovery planning [2][3][15] (See Figure 4).

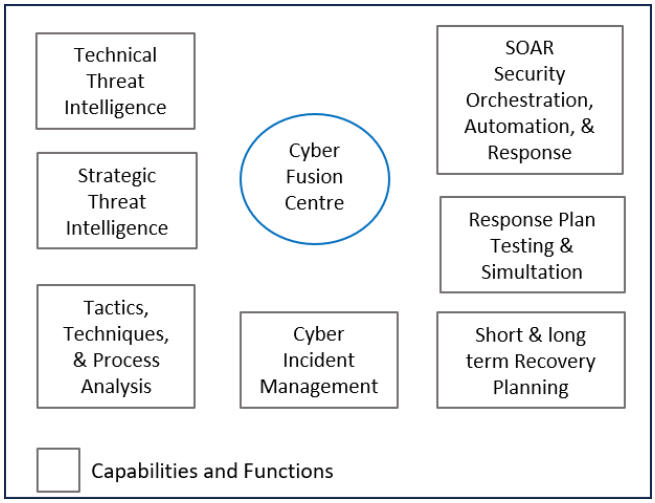

Figure 4. Intelligent Cyber Fusion Centre model [3].

III. Cyber Fusion Theory Versus Practice

The accelerated response enabled by Intelligent Cyber Fusion Centres should enable organisations to move towards proactive control and near real-time containment of cyber threats [1]-[6][10]. But Cyber Fusion Centres implemented in Australian businesses differ considerably from their theoretical counterparts.

A. *Objectives & Benefits*

Financial Services Information Sharing and Analysis Centre (FS-ISAC) is a collaborative not-for-profit venture whose mission is to "advance cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve" [8]. The 2023 whitepaper released by FS-ISAC and authored by a subcommittee of its members, provides recommendations for establishing and implementing a Cyber Fusion Centre in a bank. According to the FS-ISAC whitepaper, the CFC's primary benefit is derived from sharing information during an incident, by "synchronising response activities across different regions, business units, and other Fusion Centers." In addition, the whitepaper highlights that the CFC establishes a common language, streamlining communications between responders and leadership prior to and during security events, and improving c-suite risk reporting. The expected benefits revolve around the resultant uplift in response capability based on:

- "Standardised, repeatable, incident response and management processes;
- Enhanced transparency into tactical reactions to events;
- Dedicated, trained, and experienced incident commanders;
- Improved adherence to regulatory disclosure requirements;

  Demonstrated overall security posture to regulators/clients/and executives" [9].

B. *Fusion Centre Participants*

The FS-ISAC whitepaper on Cyber Fusion Centres (2023) describes a centralised, co-located or distributed, virtual model focused on response and incident management, where multiple areas in the business are impacted [9] (See Figure 5).

FS-ISAC recommends the core participants in the fusion centre include representatives from:

- Security Operations Centre (incl. Cyber & Technology)
- Incident & Crisis Management
- Fraud Management
- Physical Security
- Intelligence
- Third Party Management
- Communications
- Compliance, and
- Legal

A secondary group of participants are recommended to participate when an incident is relevant to their areas of responsibility. These secondary members include:

- Accounting
- Anti-Money Laundering (AML)
- Business Continuity
- Digital Protection & Forensics

 ISBN: 978-1-68558-113-8

- Data Privacy / Breach Incident Response
- Human Relations
- Group Insurance
- Internal Investigations (Insider Threat)
- Risk
- Public Relations
- Security Architecture
- Security Awareness
- Service Management (Eg Payments, Customer Service, Internet Banking), and
- Vulnerability Management [9].

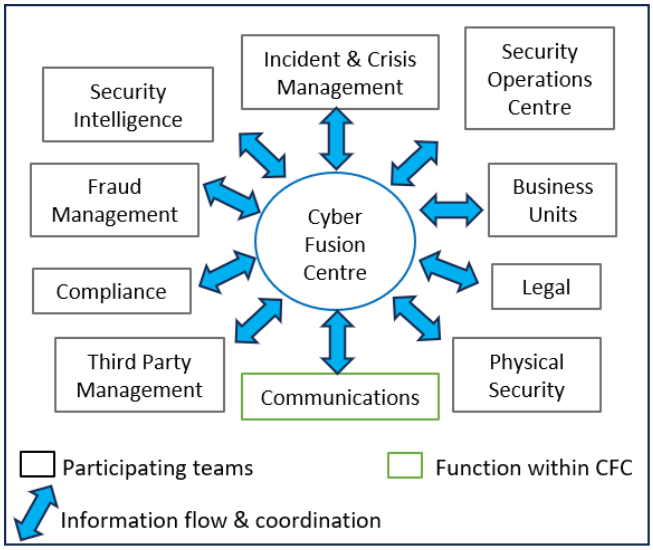

Figure 5. FS-ISAC Cyber Fusion Centre Model, based on [9].

C. Implementation Model

The FS-ISAC paper outlines the method for implementing a Cyber Fusion Centre starting with a daily check-in, where participants share observations and insights from the previous 24 hours. The purpose of the daily check-in is to facilitate collaboration between participating teams and capture the updates they provide. Participants raise items of interest, question one another, and look for common elements and themes. The coordinating CFC team documents and tracks items raised and actions involving multiple participating teams. As the CFC matures, trends and patterns may be identified and tracked [9].

IV. Implementation of Cyber Fusion Centres in Australia

The few fusion centres in Australia are concentrated in the larger banks. These organisations are highly complex, heavily regulated, and potentially lucrative targets for threat actors [4].

A. Size and complexity matters

Industry research indicates that only the big-4 banks in Australia are implementing or considering implementing Cyber Fusion Centres. In these large-scale organisations, the complexities of communicating between multiple teams who participate in cyber, fraud, and service management incident detection and response, with their different perspectives and priorities, can hamper fluid information flow. The large security departments that have evolved in these banks naturally segregate into silos, with each team focusing on their local accountabilities [2].

Two of the big-4 Australian Banks have attempted to implement cyber fusion centres. In these organisations, the CFC has played a role in bridging the gaps across disparate teams, facilitating open communications, and creating an integrated perspective for response activities. The first of the big 4 banks to implement Cyber Fusion, established a virtual capability where people from different teams across security came together to facilitate incident response. This virtual model was disbanded when the Chief Information Security Officer (CISO) who championed its creation, exited the organisation.

In another of the largest Australian banks, the CFC was established with an initial focus on facilitating information flow. The central fusion team coordinates daily communications forums each morning, with representatives from the different teams across cyber and physical security, fraud, IT service management priority incident response, crisis management, supplier management, and customer service (See Figure 6). These specialised teams have been functioning independently prior to the creation of the CFC. Coming together daily to share updates and insights on what they have seen in the previous 24 hours has facilitated greater cooperation between the teams. The CFC has been active in encouraging this cooperation, involving themselves when an incident spans multiple domains.

Beyond initial benefits elicited from the sharing of insights and improved cooperation, the value being derived from the CFC has been limited. While the non-cyber teams share their experiences openly, the core-cyber teams continue to show resistance to imparting any real information. The updates provided by these participants do not include detailed technical threat intelligence regarding the threats facing the bank, nor corresponding alerts, nor strategic threat intel showing trends, motivations and characteristics, and adversary behaviours. This is impacting the depth of situational awareness across the participants, which continues to be limited and localised. Further work is

 ISBN: 978-1-68558-113-8

needed to develop trust and a sense of shared purpose for the cyber teams.

The expected benefits from the CFC, such as accelerating threat response, are not yet being seen. The CFC has not played a role in developing SOAR capabilities, nor have they made plans to facilitate practice sessions in preparation for major or significant incidents, nor are they involved in short- and long-term recovery planning. While the CFC team supports incident management spanning multiple domains, the majority of cyber incident management continues to be accomplished locally within the specialist teams.

Observational analysis indicates that, to a large degree, the development and success of the CFC is being hindered by the inexperience of the CFC leader and their lack of knowledge and understanding of cybersecurity, fraud, and/or financial crime. In addition, progress is stymied by the absence of a rousing vision, coupled with an inability to lead diverse teams and drive organisational change through inspirational leadership.

Without a clear vision and roadmap to propel them forward, in this instance, the CFC is falling prey to operating at the task level. Continued aversion to implementing performance measures, to focus their actions on outcomes, may make it challenging for them to justify their value over time.

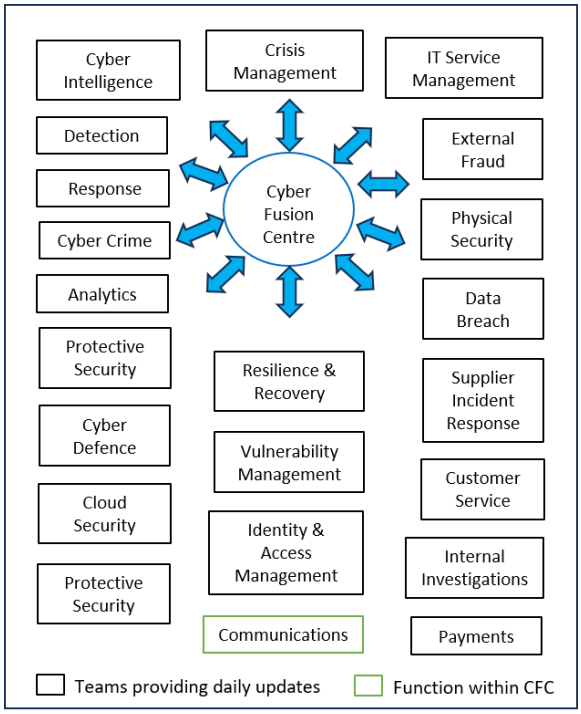

Figure 6. Cyber Fusion Centre in Australian Bank.

B. Crisis Management

In the Australian bank, where the CFC facilitates a daily standup with representatives from the areas illustrated in Figure 6, observations are discussed, insights are shared, and areas of overlap and interdependence are highlighted. Where interdependencies are more complex and broader-reaching incidents are revealed, the CFC team steps up to try to ensure an integrated response approach.

High Priority cyber incidents emerging from these collaborative sessions, whose scale of impact or potential impact exceeds an agreed threshold, are handed over to the Crisis Management Team (CMT). The CMT coordinates crisis management across IT support and operations, service management, suppliers, customer service, corporate communications, and business leaders to ensure a consistent approach. They receive tip offs from various sources, including the CFC daily standups. They have clear accountabilities and established, direct communication with senior management and the C-suite. The CFC team leans-in to provide day-to-day support to the Crisis Management Team during a crisis situation (See Figure 7).

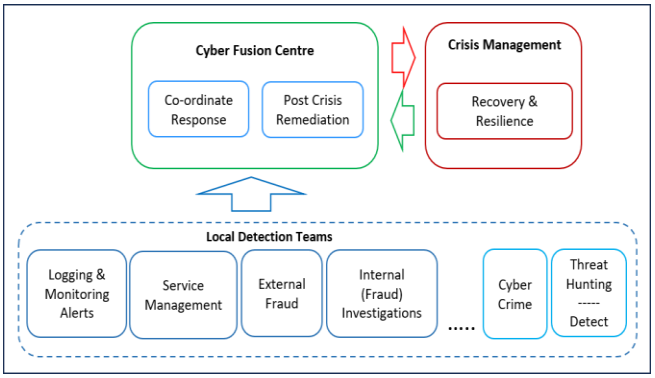

Figure 7. Fusion and Crisis Management in an Australian Bank.

C. Vulnerability Remediation

Vulnerabilities and remediation requirements identified through this bank's Crisis Management process are captured through the crisis management process. These vulnerabilities are prioritised, funded, and remediated to ensure similar situations are not repeated. Many of these vulnerabilities are known, reported and documented prior to the incident, but not prioritised or funded. These larger scale incidents, and the resultant crises, provide appropriate visibility and senior management focus to the potential risks, and the funding follows.

D. Small Scale

Smaller organisations can rely on open communications and close interpersonal relationships when coordinating their response efforts, but this is not scalable. The smaller scale organisations that were assessed in the energy and financial sectors did not see a need for a CFC, as communications and coordination during high priority incidents was straightforward. Analysis found that the

 ISBN: 978-1-68558-113-8

communications within smaller organisations, such as those within the insurance and energy sectors, is naturally more open and less arduous. With only a handful of individuals involved in incident management and cyber response, it is easy for each participant to have a deep understanding of their own area of accountability, as well as visibility across the cyber and business landscape. In these smaller organisations, there is less opportunity for information to fall through the gaps.

V. ADDRESSING THE GAP

The lack of maturity observed in the existing Cyber Fusion Centres in Australia is reflected in the benefits they deliver. These fall far short of the goal. But the level of capability uplift described in the literature is attainable. The keys to addressing the gap between Cyber Fusion Centre theory and practice can be found in the fusion models that have been most successful in military operations; the COINOPS intelligence fusion and flow model. This model highlights the need for:

1. A Shared Vision

   The COINOPS commander in the field is clear on their direction, with a strong vision of the mission objectives. The vision of a cohesive mature CFC function, that brings together every aspect of cyber: intelligence; vulnerability management; detection; response; and recovery, with technology, and customer support, for complete situational awareness, is exciting. The CFS vision needs to be clearly and inspiringly communicated from the top echelons of leadership through the CFC leader, to the analysts and response teams working day-to-day with the CFC.

2. The Right Skills and Leadership Capability

   Cyber Fusion effectiveness relies on the right mix of skills and capabilities, in the same way the COINOPS effectiveness relies on the right mix of skills for intelligence fusion and flow. The effective COINOPS platoon in the field incorporates both military specialists and professionals who understand the environment, with language and technology specialists, and intelligence analysts who generate situation awareness [11]. The platoon commander's understanding of the civilian and military context, in that moment, in the field, is crucial. Their depth of experience and capability is reflected in their ability to lead a diverse team of specialists, through challenging situations; distilling intelligence, providing direction; and retaining grasp of the goal while flexing to fit with the constantly changing circumstances [11].

   The fusion centre leader requires an equivalent level of contextual appreciation, depth of leadership capability and experience, focus on outcomes, and the ability to distill information and lead diverse teams of specialists through potentially challenging situations.

3. Clear Information Flow and Accountabilities

   The DHS Counterterrorism Fusion model illustrates how different accountable teams can be brought together into fusion centres to work more collaboratively and to facilitate information flow from state to/from national level [15]. The COINOPS model has taken this to the next level, accelerating the flow of information and intelligence through the layers of command to enable and empower the platoon commanders in the field to make informed decisions, in the moment [11]. Similarly, the effectiveness and efficacy of Cyber Fusion and Incident Response in organisations relies on clear accountabilities and fluid flow of information and intelligence, vertically and horizontally.

4. Robust Strategy and Roadmap

   Turning the Cyber Fusion Centre vision into reality relies on having a roadmap that outlines the steps to get from the current, manual, reactive reality, to the proactive, informed real-time intelligent fusion analytics and integrated response capability. This roadmap needs to include all the relevant changes needed for policies, processes, technology and people.

   Significant performance uplift can be attained by strategically utilising existing technology and intelligence already available within the organization, to facilitate situational transparency and awareness across the response teams. As it matures, CFC will be required to leverage technology for timely information flow, integrated intelligence analytics, and orchestrated response capability.

5. Practice

   Regular simulated crises will build the skills to manage large scale and broad reaching incidents, uplifting response capability and building business readiness [12][16].

6. Collaborative Working

   Utilizing capable leadership to overcome resistance to the new ways of working is the most challenging aspect of building a fusion centre. The CFC is a shared responsibility with potential benefits that span the business. Effective organisational change management, with visible

 ISBN: 978-1-68558-113-8

senior-leader sponsorship, and hands-on and capable leadership from the CFC, will inspire and encourage teams to participate, learn from one-another, build mutual trust, and share in the collective gain of fusion [3].

7. Performance Measures

Performance measures help team members to focus on the elements that make a difference. To demonstrate how the CFC can accelerate cyber threat response, performance metrics such as: the Mean Time To Detect (MTTD), Mean Time To Respond (MTTR), and Mean Time To Contain (MTTC) need to be baselined and tracked [6]. Improvements in these measures will highlight the CFC's value, as well as point to areas requiring their attention.

VII. CONCLUSION

The Cyber Fusion Centre holds great promise for organisations faced with coordinating multiple divisions and departments when responding to cyber incidents. The literature paints a picture of Cyber Fusion Centres as hubs of intelligence, knowledge, and response coordination excellence; where expertise comes together to problem solve and drive actionable outcomes. The reality is much simpler and more basic. The Cyber Fusion Centres described in the FS-ISAC whitepaper and being implemented in Australian banks, focus on basic manual and reactive response coordination through daily standups where representatives share their observations and insights with one another. While this has provided some benefit through open information sharing across teams, it is not delivering the anticipated improvements.

Building a mature intelligence-enabled cyber fusion capability and realising the associated benefits, requires visionary and strategic leadership, a broad appreciation of cyber security in all its aspects, an ability to engage and inspire cyber professionals to join-in, and a deep understand of the problems the fusion centre is addressing, along with the skills to make it happen.

REFERENCES

[1] Anomali, What is a Cyber Fusion Centre, Available from: https://www.anomali.com/blog/what-is-a-cyber-fusion-center, accessed July 2023.

[2] Cyware, What is a Cyber Fusion Center Center and how is it different from Security Operations Center (SOC)?, August 2018, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/what-is-cyber-fusion-center-and-how-is-it-different-from-security-operations-center-soc-b13a, accessed June 2023.

[3] Cyware, Building a Cyber Fusion Center, November 2020, Available from: https://cyware.com/educational-guides/cyber-fusion-and-threat-response/building-a-cyber-fusion-center-ae08/, accessed June 2023.

[4] Cyware, Why are Financial Institutions Adopting Cyber Fusion Strategies, May 2022, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/why-are-financial-institutions-adopting-cyber-fusion-strategies-57b5, accessed June 2023.

[5] Cyware, How Can You Improve Your Security Posture with Cyber Fusion?, June 2022, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/how-can-you-improve-your-security-posture-with-cyber-fusion-3afb, accessed June 2023.

[6] Cyware, How Cyber Fusion Provides 360-degree Threat Visibility? July 2020, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/how-cyber-fusion-provides-360-degree-threat-visibility-8fda, accessed June 2023

[7] D. P. Fidler, Inter arma silent leges Redux? The law of armed conflict and cyber conflict, Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press / Washington, DC 2012.

[8] FSISAC[1], Financial Services Information Sharing and Analysis Center, Available from https://www.fsisac.com/, accessed June 2023.

[9] FSISAC[2] Fusion Council, Considerations for Implementing a Fusion Operating Model in Financial Services– Whitepaper, Financial Services Information Sharing and Analysis Centre (FS-ISAC) May 2023. Available from https://www.fsisac.com/, accessed June 2023.

[10] K. L. Mclaughlin, Cybersecurity and fusion centers, The EDP Audit, Control, And Security Newsletter 2023, vol. 67, no. 4 2023, Available from: https://www.tandfonline.com/doi/pdf/10.1080/07366981.2023.2205689, accessed June 2023.

[11] A. Mishra, Synchronising Counterinsurgency Ops with Effective Intelligence, Available from: https://theforge.defence.gov.au/publications/synchronising-counterinsurgency-ops-effective-intelligence, accessed July 2023.

[12] A. Reeves and D. Ashenden, Understanding decision making in security operations centres: building the case for cyber deception technology, 2023. Available from: https://www.researchgate.net/search.Search.html?query=security+operations+centre&type=publication, accessed June 2023.

[13] S. Reveron, An introduction to National Security and Cyberspace, Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press / Washington, DC 2012.

[14] J. B. Sheldon, Toward a theory of cyber power: Strategic purpose in peace and war, Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press / Washington, DC 2012.

[15] J. E. Steiner, Needed: State-level, Integrated Intelligence Enterprises, Studies in Intelligence vol. 53, no. 3 (Extracts, September 2009), Available from: https://www.cia.gov/static/Needed-State-Level-Integrated.pdf, accessed June 2023.

 ISBN: 978-1-68558-113-8

[16] J. Steinke et al., Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research, Security and Privacy: building dependability, reliability, and trust, Multidisciplinary Security, July/August 2015, vol. 13, no.4, Available from: https://www.researchgate.net/publication/281467215_Improving_Cybersecurity_Incident_Response_Team_Effectiveness_Using_Teams-Based_Research, accessed September 2023.