Toward Better Use of Cyber Threat Models in Defence Environments

Steve Johnson, Erisa Karafili
School of Electronics and Computer Science, University of Southampton, United Kingdom
Steve.Johnson@soton.ac.uk, E.Karafili@soton.ac.uk

Abstract: Threat modelling in cybersecurity is a systematic process for identifying, analysing, and prioritising threats in a system. However, it is a highly challenging task in the defence sector, since military capabilities present a broad attack surface. This problem is compounded by the widespread use of civilian threat models, designed for specific systems or security aspects, in the defence sector, which often lack the breadth required to analyse military capabilities. In this paper, we identify gaps in state-of-the-art threat models in their ability to represent threats in the defence sector, using TEPIDOIL, a framework that captures the components required to maintain effective defence capabilities. We then present a novel framework called *Universal Defence Framework*, and demonstrate, through a case study and evaluation, that it enables the use of existing (civilian) threat models in the defence sector and addresses the identified gaps. Our evaluation showed that integrating threat models into our framework provides the broader view required to analyse threats in complex, integrated systems, as typically found in the defence sector.

Keywords: Threat Modelling, Defence, TEPIDOIL, STRIDE, OCTAVE, Cyber Kill Chain

1. Introduction

In cybersecurity, threat modelling is a crucial process for identifying how adversaries can penetrate a system and escalate attacks. It identifies system components, how they can be compromised, and helps prioritise risks that pose the greatest harm to the system. Hence, threat models are highly useful for analysing system weaknesses.

Threat modelling is a key pillar in the planning and improvement of responses to attacks in the defence sector. However, there are three key problems. First, civilian threat models are typically designed for a specific system or security aspect, e.g., Cyber Physical Systems (Valenza et al., 2022), Internet of Things (Mahlous, 2023), software systems (Sion et al., 2021), human factors (Ferro et al., 2021), and others. Thus, unable to represent the complexity of the defence sector. Second, defence environments are often defined in terms of capabilities: the ability to perform an action or to deliver a service or function. Military capabilities rely on aspects that are not fully integrated in the civilian context, e.g., logistics, doctrine. Third, civilian threat models are used in defence environments, even though they typically do not provide the breadth required to analyse military capabilities with a broad attack surface. Hence, threat modelling in defence requires a broader perspective; otherwise, it would only partially represent a capability, creating blind spots.

In this paper, we address this problem by identifying the representation gaps threat models have when used in the defence context. In particular, we evaluate these threat models against TEPIDOIL, a UK Ministry of Defence (MoD) framework that captures the components required for maintaining effective defence capabilities (MoD, 2024). To address representation gaps, we introduce a novel *Universal Defence Framework* that enables the use of civilian threat models in the defence sector and captures critical defence components and capabilities.

To identify the gaps, we analysed three threat models used in both defence and civilian contexts. We evaluate these threat models by comparing their representation capabilities with respect to TEPIDOIL, which encompasses Training, Equipment, Personnel, Information, Doctrine and Concepts, Organisation, Infrastructure, and Logistics (MoD, 2024). Vulnerabilities in any of these components can impact the delivery of capabilities. For our analysis, we selected STRIDE (Kohnfelder and Garg, 1999), OCTAVE (Alberts et al., 2003), and Cyber Kill Chain (Hutchins et al., 2011), as they are popular approaches used for threat modelling (Suhas, 2023; Naik et al., 2024). While it is challenging to provide evidence of these threat models in critical defence scenarios (due to secrecy in this sector), they are frequently emphasised in defence documentation, as recommended or useful threat models.

Our analysis confirmed that these threat models cannot represent all TEPIDOIL components. To fill these gaps, we introduced our novel *Universal Defence Framework*, which enables the application of civilian threat models in the defence sector to facilitate comprehensive analyses of military capabilities. To showcase our framework, we present a case study on a military application. This case study clearly shows that it allows threat models to represent defence aspects that could not be represented before. Our preliminary evaluation shows that our framework enhances the representation capabilities of threat models for the defence sector.

In Section 2, we present briefly the related works. In Section 3, we analyse each threat model to identify their representation gaps. In Section 4, we present our novel *Universal Defence Framework*. In Section 5, we present a case study demonstrating the application of our framework. In Section 6, we evaluate how our framework enhances existing threat models and discuss the limitations of our work. Finally, in Section 7, we conclude and provide future research directions.

2. Related works

Threat models are crucial in identifying vulnerabilities in systems and software. Threat models are generally used for civilian contexts. Valenza et al. (2022) developed a threat model and tool that takes as input a system's digital, physical, and human assets and derives how threats can propagate through the system. Mahlous (2023) quantified the severity of harm caused by threats across different asset types in an Internet of Things system, using the STRIDE threat model. Sion et al. (2021) developed a tool that analyses threats in a software system during code updates, facilitating dynamic and automated threat modelling. Ferro et al. (2021) developed STRIDE-HF, a threat model that helps analysts identify how human-factor weaknesses (e.g., a lack of understanding) can enable cyberattacks. Sgandurra et al. (2016) presented a threat model for virtualized systems.

Let us describe three state-of-the-art threat models, i.e., STRIDE, OCTAVE, and the Cyber Kill Chain, that have been used in the defence sector, with examples of this usage.

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) (Kohnfelder and Garg, 1999) was originally designed for threat modelling software systems but has since been applied to other systems. STRIDE, combined with Data Flow Diagrams (DFDs), is particularly useful for classifying threats into each of the six categories by asking, for example, 'Is there a possibility for an adversary to present as another entity to exploit this part of the system, and what threats can allow this?' (e.g., Spoofing threats). A notable implementation of STRIDE in defence is the guidance proposed by the UK Department for Science, Innovation & Technology (DSIT, 2024) for threat modelling smart-city-related technologies using STRIDE. The guidance presents four cases in which local authorities have deployed the approach to identify threats across different contexts, including IoT devices, connected safety devices, and air quality sensors.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Alberts et al., 2003) is a threat model that has three key phases. The first phase requires threat modellers to identify organisational assets in order to identify critical assets that, if compromised, have a significant impact on the business. The second phase involves identifying and analysing the components that enable crucial assets to function as expected, as well as weaknesses. Finally, the third phase requires analysts to develop countermeasures to address the identified vulnerabilities. While information on the application of OCTAVE in defence is often classified, research sponsored by the US Department of Defence (Woody, 2006) indicates that training is provided to medical teams to conduct risk assessments of healthcare systems using OCTAVE, identify and prioritise security risks, and formulate countermeasures.

Cyber Kill Chain (CKC) (Hutchins et al., 2011) is designed to decompose cyberattacks into seven phases that detail how adversaries collect the information required to conduct the attack, how an exploit is built, and how exploits are delivered. The threat model is useful for a range of scenarios. First, before a cyberattack, the CKC can be used by organisations to plan how they will manage each stage. Second, when managing a live attack, the CKC can be used to predict adversarial actions. Third, the CKC can be used to analyse why and how a cyber-attack occurred by reconstructing a series of events. A notable implementation of the CKC in defence is by the US Marine Corps, which deployed a red/blue teaming activity to test how well attacks against critical infrastructures could be defended against realistic attack scenarios (Corbo, 2022). The CKC was used to design multiple attack scenarios, in stages that mirror the progression of real attacks.

3. Analysis of threat models

In this section, we introduce TEPIDOIL and analyse STRIDE, OCTAVE, and CKC with respect to their ability to represent TEPIDOIL elements. Our analysis finds that these models cannot fully represent and analyse TEPIDOIL elements, as shown in Table 1.

TEPIDOIL is a framework that defines components that facilitate an effective military capability. A capability refers to the ability of a defence organisation to perform an action or to deliver a service or function (MoD, 2024). Each component of TEPIDOIL can introduce threats; hence, for a capability to be effective, all components must avoid significant compromise. This highlights that capability-based threat modelling must consider a broad

range of systems and components. TEPIDOIL's components can be defined as ensuring the following: (1) Training: Ensuring that individuals are proficient in conducting their responsibilities well; (2) Equipment: Ensuring the availability and effectiveness of software or physical tools that support the capability; (3) Personnel: Ensuring individuals with the correct expertise and ethical conduct can support the desired outcomes; (4) Information: Ensuring that data is only accessible by authorized parties, that it remains available and untampered by unauthorized parties, and is processed securely; (5) Doctrine and Concepts: Ensuring that military forces are guided by robust processes, frameworks, and guidelines; (6) Organisation: Ensuring that there are structures in place to facilitate defence objectives, particularly regarding management structures, and how roles interact with each other; (7) Infrastructure: Ensuring that there are structures required to aid defence objectives (e.g., buildings); (8) Logistics: Ensuring that approaches are sustainable (e.g., developing maintainable assets and tools).

Our analysis on *STRIDE* identified gaps or partial representation in seven of eight TEPIDOIL elements. In particular, (1) Training: STRIDE can model the platform used for training (e.g., Denial of Service threat: training platform can be disrupted), but key threats, such as how an individual's skill can degrade during the lifecycle of capabilities, cannot easily be derived; (2) Equipment: Software equipment can effectively be analysed in STRIDE, though, since it is information-centric, physical threats are less derivable from DFDs or analyses; (3) Personnel: STRIDE is limited in being able to derive the reasoning behind human factor errors (e.g., fatigue); (4) Information: The model is comprehensive in identifying information security threats; (5) Doctrine and Concepts: STRIDE can represent doctrine and concepts (e.g., guidelines) as assets, however, the suitability of doctrine for capabilities is not assessed; (6) Organisation: While STRIDE allows practitioners to identify information flow through the system, threats that arise from governance, for example, in a team, are not analysed by default; (7) Infrastructure: In STRIDE, components of the system are organised into boundaries (e.g., with DFDs), however, STRIDE does not often consider this from a physical point of view, though some physical implications can be analysed using denial of service or tampering categories; (8) Logistics: Threats impacting how well a capability can be sustained are challenging to derive without additional prompts.

Our analysis on *OCTAVE* found that it overall covered more elements, with two TEPIDOIL elements covered and the rest partially covered. In particular, (1) Training: The first phase in OCTAVE can identify weaknesses in the organisation, which can include those related to training, however, the documentation (Alberts et al., 2023) emphasises the assets themselves; (2) Equipment: OCTAVE identifies critical assets well, but gives less attention to specific software or physical equipment vulnerabilities than other models, e.g., STRIDE; (3) Personnel: Human-factor risks may emerge in Phase 1, but they are not strongly emphasised and can be overlooked. (4) Information: Information threats are well covered, as Phase 1 includes identifying key data assets. (5) Doctrine and Concepts: OCTAVE assesses policy and guideline compliance rather than weaknesses in doctrine itself; (6) Organisation: Risks from organisational roles and governance can be identified; (7) Infrastructure: Phase 2 analyses infrastructure supporting business functions, but mainly when tied to a crucial asset rather than as a risk source on its own; (8) Logistics: Logistics related threats (e.g., delivery capacity or timing) are not addressed by default unless analysts explicitly apply TEPIDOIL.

Our analysis on *CKC* found that it can represent three TEPIDOIL elements, partially represent two, and cannot represent three. In particular, (1) Training: CKC can place training weaknesses within an attack sequence, but it does not evaluate training threats directly, and training is rarely the primary target; (2) Equipment: Equipment attack paths can be mapped clearly through the step-by-step phases of the model; (3) Personnel: Human-factor weaknesses (e.g., exploited through phishing) can be represented, but CKC is not designed to analyse them in depth and often treats them only as attack initiators; (4) Information: The model can specify how information assets can be impacted (e.g., with the actions on objectives stage); (5) Doctrine and Concepts: Doctrine may be treated as an asset that can be attacked, but threats arising from doctrine itself receive little emphasis; (6) Organisation: Reconnaissance may capture organisational details, but CKC is less effective for deriving organisational risks than models like OCTAVE; (7) Infrastructure: The model effectively maps attacks on networks and physical architectures, including pathways to compromise; (8) CKC can illustrate disruption of logistical processes, but detailed analysis may require adaptation or explicit prompting.

Our analysis has highlighted gaps in the representation of TEPIDOIL elements in these threat models (see Table 1). Although each model can comprehensively represent the information component in TEPIDOIL (i.e., derive information-security-centric threats), analysts would require explicit prompting to consider other components (e.g., training or logistics). Without this, analysts may produce threat models that only partially represent the threats in a capability because a standardised process has not been used.

Element	*STRIDE*	*OCTAVE*	*CKC*
Training	◑	◑	✕
Equipment	◑	◑	✓
Personnel	✕	◑	◑
Information	✓	✓	✓
Doctrine and Concepts	◑	◑	✕
Organisation	✕	✓	✕
Infrastructure	◑	◑	✓
Logistics	✕	◑	◑

Table 1: Gaps summary. ✕ = not typically captured; ◑ = requires explicit consideration; ✓ = well captured by default.

4. Proposed approach: Universal Defence Framework

In this section, we introduce our *Universal Defence Framework*, designed to enable analysts to comprehensively analyse military capabilities using a threat model of their choice to identify threats. Our framework is a general extension that enhances existing models. This addresses a key limitation of civilian threat models highlighted in Section 2: they are not optimal for analysing capabilities by default. Note that our proposed approach is a general framework that enhances most threat models, rather than addressing specific limitations in STRIDE, OCTAVE, or CKC, which provide different functionalities.

Our framework has four main concepts: *capabilities*, *functions*, *assets*, and *failure modes*. A capability is the ability to perform an action or deliver a service or function (broad view). Functions are the aspects that enable a capability to be effective (more descriptive). Assets are the people, processes, and technologies required for functions to operate (granular details). Finally, failure modes denote states of assets or functions (e.g., compromised, degraded, or normal).

Our framework, presented in Figure 1, consists of four key stages, each with associated processes. In Phase 1, analysts contextualise further analysis to the capability by (i) defining the capability, (ii) defining the functions that enable the capability, (iii) defining failure modes in the functions, and (iv) defining unacceptable compromises to the capability. In Phase 2, analysts identify the assets involved in making the functions work by (i) identifying TEPIDOIL assets (people, processes, and technologies) required for each function from Phase 1, and (ii) defining failure modes for every asset. In Phase 3, analysts identify threats to assets by (i) selecting the threat model(s), e.g., STRIDE, OCTAVE, CKC, etc., (ii) applying the threat models(s) to each asset from Phase 2 to identify threats, and (iii) evaluating how each threat against an asset would cause a failure mode in the asset and the functions that depend on the asset. Finally, in Phase 4, analysts (i) evaluate the impacts of failure modes triggered in functions (from Phase 3) on the capability, considering the conditions from Phase 1, Process (iv).

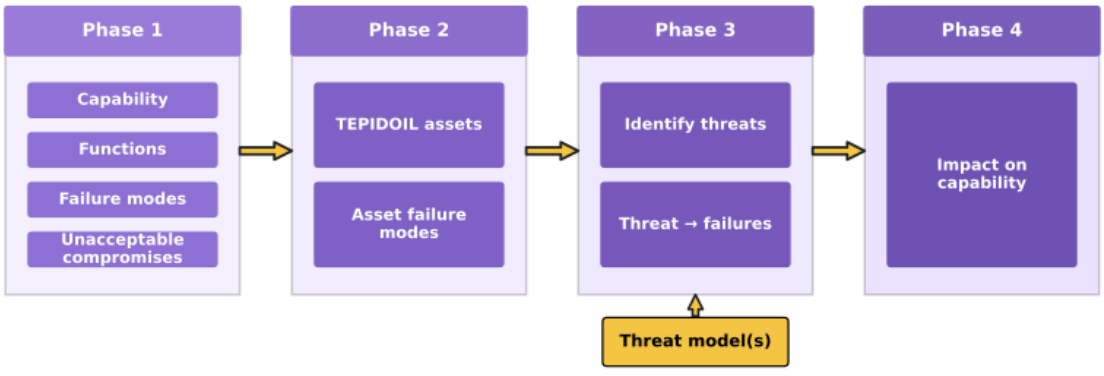

Figure 1: Universal Defence Framework.

5. Case study

In this section, we demonstrate the application of our framework through a case study, which is a conceptual example of a capability presented in an MoD advisory.

Let us introduce the case study (MoD, 2025). During missions, military forces are delivered supplies (e.g., power and medical aid) via Unmanned Aerial Vehicles (UAVs). To enable personnel to collect their supplies, they must be able to track the UAV and receive relevant delivery information via military software on their mobile phones. A capability refers to the ability to perform an action or to deliver a service or function. Hence, in our case study, capability refers to the ability to track the UAV effectively using software, and threats to TEPIDOIL elements can affect the execution of this capability.

We now demonstrate how our framework can be applied to this capability, showing how the processes in our proposed framework align with threat models such as STRIDE.

Phase 1: Contextualise to the capability.

- *Process 1: Define the capability:* Software must allow military personnel to track the UAV in conflict environments reliably.
- *Process 2: Define functions that enable the capability:* (1) Authenticate users [F1], (2) Allow delivery tracking [F2].
- *Process 3: Define failure modes in the function:* For simplicity, all functions will have the following failure modes: Normal (N), Degraded (D), Compromised (C).
- *Process 4: Define unacceptable compromises to the capability:* (1) Death of military personnel [UC1], (2) Delivery information about supplies is disclosed [UC2].

Phase 2: Identify assets.

- *Process 1: Identify TEPIDOIL assets (people, processes, technologies) required for functions to work:* Simplified example (in-depth analysis can include more assets):
    - For F1:
        - People: Military personnel (Personnel)
        - Processes: Access token must be issued (Equipment)
        - Technologies: Mobile phone (Equipment); software (Equipment)
    - For F2:
        - People: Military personnel (Personnel)
        - Processes: Updates to delivery progress (Equipment)
        - Technologies: UAV telemetry (Equipment); software (Equipment)
- *Process 2: Identify failure modes for assets:* For simplicity, modes for all assets are *normal (N)*, *degraded (D)*, or *compromised (C)*, but these can be specified further.

Phase 3: Identify threats.

- Process 1: Select the threat model(s): STRIDE
- *Processes 2 and 3: apply threat model to each asset (from Phase 2) to identify threats, and for each threat evaluate how it can cause (→) a failure mode in the asset and a failure mode in the functions that depend on the asset.*
    - Military personnel:
        - Spoofing: Adversaries obtain user credentials via a successful phishing email and enter the software using those details. [Military personnel: C → F1:C, F2:C].
        - Information disclosure: Military personnel reveal UAV delivery information to unauthorised parties. [Military personnel: C → F2:C].
    - Access tokens:
        - Spoofing: Adversaries impersonate military personnel by replacing tokens. [Access token: C → F1:C, F2:C]
        - Tampering: Adversaries modify tokens. [Access token: C → F1:C, F2:C]
        - Information disclosure: Adversaries extract tokens from data stores. [Access token: C → F1:C, F2:C]
    - Mobile phone:
        - Spoofing: Adversaries steal the mobile phone to imitate military personnel. [Mobile phone: C → F1:C, F2:C]
        - Denial of service: Damage to the device prevents personnel from using tracking software. [Mobile phone: D → F1:D, F2:D]

- Software (UAV tracking software):
  - Tampering: Adversaries modify software code. [Software: C → F1:C, F2:C]
  - Information disclosure: Adversaries access software artefacts stored on a programmer's device. [Software: C → F1:C, F2:C]
  - Denial of service: The app malfunctions. [Software: C → F1:C, F2:C]
  - Elevation of privilege: Poor authentication processes result in personnel accessing delivery information outside of their role. [Software: C → F1:C, F2:C]
- UAV telemetry:
  - Spoofing: Adversaries fabricate telemetry [UAV telemetry: C → F2:C]
  - Denial of service: Adversaries jam telemetry, preventing UAV tracking. [UAV telemetry: C → F2:C]
- Updates to delivery progress:
  - Tampering: Adversaries modify delivery updates. [Updates to delivery progress: C → F2:C]
  - Repudiation: There is no auditing for personnel who updated the delivery progress. [Updates to delivery progress: C → F2:C]
  - Denial of service: There are delayed updates, hindering prompt updates [Updates to delivery progress: D → F2:D]

Phase 4: Analyse impacts on the capability.

- *For each function compromised, analyse impacts on the capability, considering unacceptable conditions specified in Phase 1, Process (iv).*
  - All threats that compromise the crucial assets have resulted in compromised/degraded functions, e.g., C → F1:C, C → F2:C, C → F1:D, or C → F2:D.
  - For simplicity, threats are abstracted, but every threat identified can be analysed for the impact on the capability, e.g.,
    - F1 compromised [F1:C], e.g., can result in threat actors masquerading as genuine users, resulting in UC2 (compromised capability).
    - F1 degraded [F1:D], e.g., can result in personnel not being able to authenticate, resulting in UC1 (compromised capability).
    - F2 compromised [F2:C], e.g., can result in delivery information being disclosed, resulting in UC1/UC2 (compromised capability).
    - F2 degraded [F2:D] e.g., can result in UC1 or UC2 (compromised capability).

Our case study shows how our proposed framework can be applied to comprehensively analyse defence capabilities: in Phase 1, we defined the capability (e.g., the ability to track the UAV), functions that enable the capability (e.g., software should allow tracking), and unacceptable compromises (e.g., death of military personnel); in Phase 2, we identified TEPIDOIL assets required for functions to be executed (e.g., UAV telemetry); in Phase 3, we used STRIDE to identify threats to assets (e.g., adversary jamming of UAV telemetry) and the impact on functions (e.g., military personnel can no longer view accurate delivery information); and in Phase 4, we analysed how compromised functions can lead to unacceptable consequences (e.g., the death of military personnel) that compromise the broader capability.

6. Evaluation and discussion

Let us discuss the additional features that our proposed framework provides compared with using threat models alone (see Table 2 for a summary). To begin, STRIDE, OCTAVE, and CKC are not contextualised with respect to what a capability aims to achieve. Hence, they primarily elicit threats and deconstruct attacks, without a strong link to capabilities. Our framework enables all analyses to be linked to the functions a capability aims to achieve. In addition, STRIDE, OCTAVE, and CKC provide limited guidance on what must be maintained for capabilities to be effective (though OCTAVE does so in part with respect to organisational security objectives). In our framework, we explicitly prompt analysts to define unacceptable compromises, thereby enabling analysis of the impacts of threats on the broader capability. Furthermore, STRIDE, OCTAVE, and CKC do not explicitly focus on analysing TEPIDOIL components, which is required for a comprehensive analysis of military capabilities. This can result in analysts missing crucial threats and thus creating threat models that can only partially represent a capability (creating blind spots). In our framework, we explicitly prompt analysts to identify the TEPIDOIL assets (people, processes, and technologies) that enable a capability before threat analysis. Moreover, STRIDE, OCTAVE, and CKC do not explicitly prompt analysts to delineate failure modes in assets and functions that enable

capabilities. Our framework is designed to prompt analysts to specify failure modes for both assets and functions, and to explain how a failure in an asset can cause a failure in a function, thereby compromising a capability.

Aspect	*STRIDE*	*OCTAVE*	*CKC*	*STRIDE/OCTAVE/CKC + Universal Defence Framework*
Explicit definitions of the capability underpin threat analysis.	✕	◑	✕	✓
Analyses the impact of threats on the capability based on defined unacceptable compromises.	✕	◑	✕	✓
Explicit focus on analysing TEPIDOIL components (often found in capabilities).	✕	✕	✕	✓
Explicit definitions of failure modes for assets and functions.	✕	◑	✕	✓

Table 2: Comparison of features. ✕ = not addressed; ◑ = partially addressed; ✓ = addressed.

Integrating TEPIDOIL components into our framework can broaden the perspective applied to threat modelling. That broader view is often crucial when analysing threats in complex, integrated systems, as found in the defence sector. Table 3 shows that our proposed framework serves as a standardised extension that integrates threat models to comprehensively analyse capabilities.

Model	*STRIDE/OCTAVE/CKC + Universal Defence Framework*
Training	✓
Equipment	✓
Personnel	✓
Information	✓
Doctrine and Concepts	✓
Organisation	✓
Infrastructure	✓
Logistics	✓

Table 3: Summary. ✕ = not typically captured; ◑ = requires explicit consideration; ✓ = captured by default.

Our work has two main limitations. First, we did not address the specific TEPIDOIL limitations of STRIDE, OCTAVE, and CKC identified in Section 2 by extending any specific model. However, our framework has a broad scope for the types of threat models that can be integrated, as it is generally applicable. Second, our work presents a case study using STRIDE but does not address how to resolve conflicts between processes already provided in threat models (e.g., OCTAVE) and those in our framework.

7. Conclusion and future work

In this paper, we address a key problem in threat modelling in defence environments. In particular, civilian threat models are widely used in defence; however, they typically do not provide the breadth required to analyse military capabilities that have a broad attack surface. In our paper, we evaluated state-of-the-art threat models used in both defence and civilian contexts to identify gaps in their ability to capture defence aspects. Our comparative analysis, using the TEPIDOIL framework for defence capabilities, found that threat models were unable to capture TEPIDOIL aspects. To address this problem, we introduced the *Universal Defence Framework*, a novel approach that enables existing threat models to conduct comprehensive, rigorous analyses of capabilities. We presented a case study to demonstrate how our framework can be applied and have evaluated it against the use of threat models alone. Furthermore, our evaluation highlighted that explicit prompting within our framework to define TEPIDOIL assets (people, processes, and technologies) provides the broader view required when analysing threats in complex, integrated systems, as typically found in the defence sector.

An interesting research direction is to develop a prioritisation scheme to help select threats that cause the greatest harm to the capability. This prioritisation scheme can specify how to prioritise assets prior to the threat analysis. To broaden the scope of application, we plan to deploy the proposed approach in a more in-depth case study, including the use of OCTAVE and CKC. Another interesting future work is to collect feedback from defence stakeholders on the usability of our framework. Furthermore, we plan to develop guidance on resolving conflicts arising from integrating multiple threat models into our *Universal Defence Framework*.

Acknowledgements

This work was supported by the EPSRC and MOD Centre for Doctoral Training in Complex Integrated Systems for Defence and Security [EP/Y034848/1]. Erisa Karafili was partially supported by the UKRI HetMEPS project (UKRI257).

Ethics declaration

Ethics clearance was not required for this research.

AI declaration

Grammarly was used for checking spelling/grammar errors.

References

Alberts, C., Dorofee, A., Stevens, J., and Woody, C. (2003) Introduction to the OCTAVE Approach, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Corbo, A. (2022) Red Team: Reserve Marines Simulate Cyberspace Attackers in Exercise Cyber Yankee 22, United States. Available at: https://www.marines.mil/News/News-Display/Article/3079808/red-team-reserve-marines-simulate-cyberspace-attackers-in-exercise-cyber-yankee/ (Accessed: 2 February 2026).

Department for Science, Innovation and Technology (2024) Conducting a STRIDE-based threat analysis, GOV. Available at: https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/conducting-a-stride-based-threat-analysis (Accessed: 2 February 2026).

Ferro, L.S., Marrella, A., and Catarci, T. (2021) A human factor approach to threat modeling, in HCI for Cybersecurity, Privacy and Trust: Third International Conference, HCI-CPT 2021, pp. 139–157.

Hutchins, E.M., Cloppert, M.J. and Amin, R.M (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), p.80.

Kohnfelder, L. and Garg, P. (1999) The threats to our products, Microsoft. Available at: https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx (Accessed: 22 January 2026).

Mahlous, A.R. (2023). Threat model and risk management for a smart home IoT system. Informatica, 47(1), pp. 51–64.

Ministry of Defence (2024) Defence Acquisition Safety Policy (JSP 376), Version 1.1. Available at: https://assets.publishing.service.gov.uk/media/664207e7993111924d9d3331/JSP_376_-_Defence_Acquisition_Safety_Policy__v_1.1_.pdf (Accessed: 3 February 2026).

Ministry of Defence (2025) Cyber Security Advisory: Managing tensions between security, safety, and human factors requirements analyses, GOV. Available at: https://www.gov.uk/government/publications/managing-tensions-between-security-safety-and-human-factors/cyber-security-advisory-managing-tensions-between-security-safety-and-human-factors-requirements-analyses (Accessed: 2 February 2026).

Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., and Song, J. (2024) A comparative analysis of threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN, in The International Conference on Computing, Communication, Cybersecurity & AI, pp. 271–280.

Sgandurra, D., Karafili, E., and Lupu, E. (2016) Formalizing threat models for virtualized systems. In IFIP Annual Conference on Data and Applications Security and Privacy. Cham: Springer International Publishing, pp. 251-267.

Sion, L., Van Landuyt, D., Yskout, K., Verreydt, S., and Joosen, W. (2021) Automated threat analysis and management in a continuous integration pipeline, in 2021 IEEE SecDev, pp. 30–37.

Suhas, K.S. (2023) Evaluation of threat models, International Journal for Research in Applied Science and Engineering Technology, Vol. 11(3), pp. 809–813.

Valenza, F., Karafili, E., Steiner, R.V., and Lupu, E.C. (2022) A hybrid threat model for smart systems. IEEE Transactions on Dependable and Secure Computing, 20(5), pp. 4403–4417.

Woody, C. (2006) *Applying OCTAVE: Practitioners report*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. Available at: https://www.sei.cmu.edu/documents/2102/2006_004_001_14675.pdf (Accessed: 2 February 2026).