Ethical Cybersecurity Dashboard to Aid Policy Making and Cyber Deterrence Strategies In the UK

Sadie Wise

Student Number: 21019207

Supervised by: Prakash Chatterjee

MSc Data Science

2024/25

# Abstract

The rise in state-sponsored cyber operations and advanced persistent threats poses significant challenges for national security, requiring policy responses that balance operational objectives with ethical responsibility. This project explores the connection between cybersecurity strategy, deterrence theory, and ethical governance, with a focus on UK cyber policy. This project develops and evaluates a decision-support dashboard informed by real-world frameworks, including NIST Cybersecurity Framework and UK National Cyber Security Centre guidance (NCSC). The study incorporates qualitative ethical reasoning with quantitative risk modelling, enabling the assessment of policy intents across simulated cyber incident scenarios. By grounding technical decision-making in transparent ethical criteria, the research demonstrates how structured tools can enhance clarity, accountability, and stakeholder engagement in cyber deterrence planning. The findings highlight the importance of multidisciplinary approaches in addressing the complex trade-offs inherent in modern cybersecurity policymaking.

Contents

[Abstract 2](#_Toc206603219)

[Chapter 1: Introduction 4](#_Toc206603220)

[Context 4](#_Toc206603221)

[Rationale 4](#_Toc206603222)

[The Problem 4](#_Toc206603223)

[Aims and Objectives 5](#_Toc206603224)

[Aims 5](#_Toc206603225)

[Objectives 5](#_Toc206603226)

[Structure of the Report 5](#_Toc206603227)

[Chapter 2: Research and Literature review 6](#_Toc206603228)

[Introduction 6](#_Toc206603229)

[Ethical Hacking and Unintended Consequences 6](#_Toc206603230)

[Cyberwarfare Policies and Strategic Doctrine 7](#_Toc206603231)

[Legal and Ethical Constraints in Cyber Operations 7](#_Toc206603232)

[Current Cybersecurity Risk Landscape in the UK 7](#_Toc206603233)

[Research Gap and Theoretical Contribution 8](#_Toc206603234)

[Chapter 3: Methodology and Proposed Artefact 8](#_Toc206603235)

[Proposed Artefact 8](#_Toc206603236)

[Research Design 9](#_Toc206603237)

[Chapter 4: Dashboard and system development 9](#_Toc206603238)

[Introduction 9](#_Toc206603239)

[System Architecture and Design Rationale 9](#_Toc206603240)

[Why Streamlit? 9](#_Toc206603241)

[Key Components and Features 10](#_Toc206603242)

[Technical decisions and tools 10](#_Toc206603243)

[Integration of Risk Modelling and Ethical Guidance 11](#_Toc206603244)

[Chapter 5: Testing and Evaluation 11](#_Toc206603245)

[Chapter 6: Conclusion and Recommendations 11](#_Toc206603246)

[References 11](#_Toc206603247)

# Chapter 1: Introduction

## Context

In an era where digital technologies underpin critical national infrastructure (CNI), cybersecurity has emerged as a defining concern for national security policy (Montasari, 2023). The United Kingdom (UK) faces rising threats from state-sponsored actors and cybercriminals who target its digital backbone—energy, healthcare, communications, and transport (Ghafur *et al.*, 2019). In response, governments are exploring offensive cyber deterrence strategies as tools of conflict prevention and power projection (Cornish, 2021). Yet, as these operations grow more sophisticated, so do the ethical and legal questions surrounding them (Helkala *et al.*, 2022). This project aims to connect cybersecurity policy, ethical risk evaluation, and a decision support system design. With aims to focus on how cyber deterrence frameworks should consider their impact on CNI and civilians specific to the UK.

## Rationale

While existing strategies explore deterrence from a technical and strategic standpoint, few offer structured means for evaluating their ethical implications (Sexton, 2016). Offensive cyber operations carry the risk of unintended harm, disrupting vital services or violating international norms (Chua *et al.*, 2019). The absence of comprehensive decision-support tools in this domain has left policymakers with limited mechanisms to forecast risks, weigh ethical trade-offs, or ensure accountability (Thornton and Miron, 2019). This project addresses that gap by proposing a dashboard that integrates simulation, ethical evaluation, and legal alignment—helping ensure that offensive cyber deterrence is applied with foresight and responsibility.

## The Problem

Current cyber deterrence policies in the UK lack a consistent method for assessing their ethical and operational risks—especially regarding effects on CNI and civilian wellbeing (Cornish, 2016). Without such mechanisms, policymakers may inadvertently approve actions that create disproportionate harm or strategic instability. This project aims to develop a decision support system that evaluates offensive cyber strategies prior to execution, ensuring that ethical considerations are integrated alongside strategic and legal frameworks. This is applicable to a variety of people and organisations and is designed to simplify this process for users.

The scope of this work includes:

* Designing a risk assessment model tailored to cyber deterrence in the UK.
* Building a simulation dashboard to visualise consequences under varying scenarios.
* Reviewing literature across ethical hacking, cybersecurity law, and cyberwarfare.
* Testing the framework using historical and hypothetical scenarios.

## Aims and Objectives

Aims  
To design and implement an ethical cybersecurity dashboard that enables UK policymakers whether that is within small and medium organisations, large organisations, public sector or professionals to evaluate offensive cyber deterrence strategies, weighing operational benefits against ethical and legal risks. This is designed to be subjective and transferable, aiming to resolve the blurred lines and understandings in a fast-moving environment.

Objectives

* Develop a simulation dashboard to visualise the impact of policies and cyber deterrence strategies on CNI and civilians.
* Create a custom risk register that models the trade-offs between risk and reward.
* Propose policy mechanisms that reduce ethical and strategic risks.
* Align the framework with UK and international cybersecurity laws and guidelines.
* Evaluate the framework’s effectiveness through scenario-based testing using past reports.

## Structure of the Report

This dissertation is organised into six chapters, each building progressively toward the design and validation of an ethical decision support framework and dashboard for UK cyber deterrence strategy:

Chapter 1: Introduction  
Establishes the context, rationale, scope, and objectives of the study. It outlines the motivation for developing an ethically grounded cybersecurity framework and introduces key guiding questions.

Chapter 2: Research  
A literature review that critically examines existing research on ethical hacking, cyberwarfare policies, legal constraints, and current cybersecurity risk in the UK. This chapter identifies gaps and informs the theoretical basis of the proposed system.

Chapter 3: Methodology and proposed artefact  
Detail the structured approach used to develop the simulation dashboard. Includes justification for scenario-based testing, simulation techniques, and ethical analysis.

Chapter 4: Dashboard and System Development  
Describes the design and implementation of the ethical decision support dashboards. Outlines key components, technical decisions, and integration points between risk modelling and ethical guidelines.

Chapter 5: Testing and Evaluation  
Presents the evaluation of the framework against realistic scenarios drawn from government reports. Discusses its effectiveness in forecasting ethical risks and offers insights from performance metrics and policy relevance.

Chapter 6: Conclusion and Recommendations  
A critical analysis on the framework created. Summarises key findings, reflects on limitations, and proposes future directions for policy, research, and system improvements.

# Chapter 2: Research and Literature review

### Introduction

The growing prevalence of sophisticated cyber threats has elevated cybersecurity from a purely technical concern to a matter of national strategy and governance. The United Kingdom (UK), like other technologically advanced nations, faces the challenge of protecting critical infrastructure, private industry, and citizens while upholding democratic values and legal obligations. Cyber deterrence policies must therefore reconcile operational effectiveness with ethical responsibility and legal legitimacy.

This literature review critically examines four domains relevant to UK cyber deterrence, ethical hacking, cyberwarfare policy, legal and ethical constraints, and the current UK cyber risk landscape, in order to establish a foundation for the proposed ethical decision-support dashboard. While each domain has been extensively studied, research tends to remain resteicted, limiting its applicability in fast-moving operational environments. The contribution of this review is to demonstrate how these insights can be synthesised into an integrated decision-support tool.

### Ethical Hacking and Unintended Consequences

Ethical hacking, often referred to as penetration testing or red-teaming, has been widely studied as a defensive practice. Chua et al. (2019) highlights that while defensive countermeasures may be ethically justified, they frequently generate collateral harm, such as the unintended disruption of legitimate systems and services. This challenge becomes particularly acute when automated countermeasures are deployed at scale, as indiscriminate blocking of traffic can harm innocent users.

Floridi (2019) situates these dilemmas within the broader field of information ethics, noting a persistent gap between high-level ethical principles and operational practices in cybersecurity. For example, aggressive monitoring for malicious traffic may help prevent breaches but risks eroding privacy and civil liberties.

Although these works identify the moral hazards associated with ethical hacking, the majority of contributions remain theoretical. Few studies translate ethical concerns into operational guidance that practitioners can use in real time. As a result, decision-makers lack practical tools for embedding ethical safeguards during live cyber operations. The proposed ethical decision-support dashboard seeks to fill this gap by providing built-in ethical “red flags” and scenario testing to prevent unintended harm before countermeasures are deployed.

### Cyberwarfare Policies and Strategic Doctrine

UK cyber policy is increasingly framed within the logic of deterrence, drawing on both defensive resilience and the possibility of offensive retaliation. Cornish (2016, 2021) analyses the UK’s evolving doctrine, with particular attention to proportionality, necessity, and escalation control. Skingsley (2023) explores the UK’s integration into NATO’s collective cyber deterrence posture, stressing the role of ambiguity over offensive capabilities in maintaining strategic balance.

Nevertheless, policy discourse often remains abstract. Devanny (2020) highlights the political and diplomatic risks of offensive operations, warning that short-term advantages may create long-term instability. The challenge is magnified in crisis conditions, where decision-makers must act rapidly on incomplete information. While doctrines emphasise proportionality and escalation management, operationalising these principles under pressure is far from straightforward.

Few studies provide mechanisms for translating doctrine into practice. For example, what constitutes a proportionate response when critical infrastructure is threatened? How should uncertainty in attribution influence escalation decisions? Existing literature rarely offers tools for testing doctrine under dynamic conditions. The proposed dashboard addresses this by embedding strategic doctrines into live simulations, enabling policymakers to evaluate policy trade-offs interactively and ethically under varied threat scenarios.

### Legal and Ethical Constraints in Cyber Operations

Legal knowledge on cyber operations emphasises sovereignty, proportionality, and attribution as major challenges. Thornton and Miron (2019) argue that attribution is particularly problematic, as technical uncertainty undermines the ability to lawfully justify retaliatory actions. Sovereignty remains contested, with some states treating network penetration as a breach of international law while others frame it as espionage, tolerated albeit unwelcome in global politics.

Helkala et al. (2022) expand this discussion into the emerging field of AI-assisted cyber operations, highlighting the absence of clear accountability frameworks. If an autonomous cyber defence system deploys countermeasures that inadvertently cause civilian harm, questions of liability arise: should responsibility rest with the operator, developer, or state? This ambiguity risks undermining trust in automated systems.

From a normative perspective, Himma (2008) cautions that legal compliance alone is insufficient for ethical legitimacy. Laws may lag behind technological change, and actions that are lawful can still be ethically problematic if they cause disproportionate harm. As this research is 17 years old, some may argue it is out of date to use as an argument however, the theories and point still stays the same and it is just as relevant now as it was when first published.

The existing literature therefore provides a strong legal foundation but lacks operational mechanisms that merge legal thresholds with strategic and ethical considerations. The proposed decision-support dashboard seeks to bridge this gap by incorporating legal guardrails directly into its recommendation outputs, ensuring that operational decisions remain both lawful and ethically defensible.

### Current Cybersecurity Risk Landscape in the UK

Studies on the UK’s cyber threat profile highlight vulnerabilities in critical infrastructure and public services. Sexton (2016) and Stoddart (2016) describe the growing risks posed by hostile state actors and organised criminal groups, particularly in energy, healthcare, and finance. Montasari (2023) analyses the UK’s adoption of “active cyber defence” where collaboration between government and industry seeks to pre-empt attacks through collective monitoring and disruption.

The healthcare sector offers a particularly stark case. Ghafur et al. (2019) document the effects of cyber incidents on healthcare delivery, showing how operational disruption spreads to supply chains and emergency services. The WannaCry ransomware attack of 2017, though technically unsophisticated, caused significant disruption within the NHS due to outdated systems and inadequate contingency planning.

These studies provide valuable situational awareness, yet they are largely static. Risk assessments are typically snapshots in time, documenting threats retrospectively or forecasting in broad terms. They do not provide interactive tools for modelling how risks evolve under different scenarios.

### Research Gap and Theoretical Contribution

Across the four domains reviewed, a common limitation emerges: existing research provides valuable insights into ethics, doctrine, law, and risk, but each remains restricted. Ethical theory rarely translates into operational tools; strategic doctrine is described abstractly but not tested in practice; legal analysis identifies constraints but does not integrate them with operational decision-making; and risk assessments provide static descriptions rather than dynamic simulations.

This division leaves policymakers and practitioners without an integrated framework to guide decisions in real time. The proposed ethical decision-support dashboard addresses this by:

1. Embedding ethical safeguards into live simulation environments to anticipate unintended consequences.
2. Operationalising cyberwarfare doctrines for scenario-based testing of proportionality and escalation management.
3. Integrating legal constraints into automated recommendation outputs.
4. Using dynamic UK cyber risk data to contextualise policy responses.

The theoretical contribution lies in synthesising these perspectives into a single, user-facing tool that supports transparent, accountable, and adaptive decision-making. By operationalising abstract insights into a practical dashboard, this research responds to calls in the literature for more integrated approaches to cyber governance and deterrence.

# Chapter 3: Methodology and Proposed Artefact

## Proposed Artefact

The proposed artefact for this project is an interactive ethical cybersecurity dashboard built using Streamlit. It is intended to assist in the UK's decision-making process on cyber deterrent measures. It combines ethical risk analysis, scenario-based simulations, and real-time data visualisation to assess the moral and strategic implications of various policy goals. Policymakers or analysts can investigate the effects of cyber incidents like infrastructure attacks or data breaches and obtain customised strategic guidance with the use of user-friendly inputs. To effectively display information, the dashboard also includes elements like a risk register, policy reference tables, and visual tools. By bridging the gap between technological danger assessments and ethical foresight, its form guarantees accessibility and scalability and provides a useful decision support tool based on real-world.

## Research Design

This research design follows a design science methodology, combining exploratory research, ethical analysis and technical implementation to develop a functional decision support artefact.

The project begins with a problem identification phase, recognising the growing complexity of cyber threats and ethical challenges policy makers face when formulating cyber deterrence strategies. A literature review is used to ground the project in existing frameworks and policies and reports and to define key policy intents and risk dimensions.

The design then shifts to a practice led, artefact driven approach where requirements are informed by both theoretical insight and practical gaps in current policy tools. The core of this project is the development of the Streamlit dashboard that integrates ethical risk modelling, simulation and visualisation.

Because the evaluation component is integrated into the artefact itself, users can apply various policy intents, simulate real-world cyber scenarios, and get dynamic ethical and strategic feedback. Instead of statistical validation, this encourages constructive evaluation.

Overall, the research design combines quantitative data interaction (risk scoring and simulation) with qualitative reasoning (ethical impact assessment), demonstrating an applicable and multidisciplinary methodology appropriate for policy innovation.

# Chapter 4: Dashboard and system development

## Introduction

This Chapter presents technical development of the artefact. The dashboard was developed using python and Streamlit, with focus on interactivity, usability and alignment with real world cybersecurity and policy frameworks. It functions as both a technical artefact and a conceptual bridge between cyber risk analysis and ethical governance. Its design enables users to explore hypothetical threat responses in a controlled, informative environment, making it an ideal tool for policy evaluation, stakeholder engagement, and academic discussion.

## System Architecture and Design Rationale

The dashboard architecture is modular, with a tabbed layout that separates core functionality into multiple components. Each module operates independently but draws on shared input and logic, supporting a scalable and maintainable design. This layout ensures clarity for users navigating between data sources, scenario exploration and output interpretation.

## Why Streamlit?

Streamlit was selected as the core development framework due to its balance between simplicity, speed and interactivity. Unlike traditional web development stacks or heavier dashboard tools like Dash or Power BI, Streamlit allows for rapid prototyping using python, with minimal setup and no need for in-depth front-end knowledge like HTML or Javascript. Streamlits integration with Python libraries like Pandas and Plotly make it suitable for handling data-driven tasks like risk modelling, scenario simulation, and visualisation. Additionally, as an open-source framework with growing community support, it provides scalability for future development or integration into institutional platforms, making it a future proof choice for a research artefact focused on usability, accessibility and stakeholder engagement.

## Key Components and Features

The design of the dashboard, as discussed previously needs clear goals regarding its functionality. Multidimensionality, accessibility, ease of use and extensibility were imperative components to incorporate.

Multidimensionality – A dashboard is made up of a collection of several visualisations that the user can combine to increase productivity. Each visualisations size and type needed to be carefully considered.

Accessibility – Users should be able to access the dashboard as readily as possible. As a result, it should have the fewest hard dependencies feasible with regard to the operating system, installed system and device type.

Ease of use- Ease of use represents a significant non-functional necessity that must be met from the viewpoint of the end user. End users, in general, should have access to all software required, with documentation though the dashboard should be made so that the user may interact with it with or without any prior assistance.

Extensibility – Finally, an extensible framework should be used when creating said dashboard so that future modifications can be made with minimal effort and without needless technological hindrances.

Some key features of the dashboard include:

Sidebar input panel - An input is collected via the sidebar that allows users to define the context of threat scenarios, adjust attack severity via a slider and choosing one of ten policy intents based on strategic goals.

Simulation engine – Upon user input, the dashboard dynamically processes the data and returns a customised policy evaluation, mapping severity and intent to a predefined ethical and strategic response using logic functions. This bridges risk modelling with ethical interpretation.

Editable risk register – Users can view and edit an excel based risk register. Once downloaded, this allows for real time interaction and modification for ongoing policy risks. There is an example risk register on the dashboard to refer to with guidance also available.

Visualisation tools - Key technical decisions include pandas for data handling and plotly for interactive visualisation. This supports insight generation through visual storytelling.

## Technical decisions and tools

* Python and Streamlit were selected for their accessibility, flexibility and development capabilities.
* Pandas enables excel integration, data manipulation and scoring logic.
* Session state logic allows temporary memory of user actions, enabling a simulation to persist across tabs.
* Markdown and user interface (UI) design were used to structure content and improve interpretability of ethical guidelines.

The session is designed for local or cloud development, ensuring adaptability for academic demonstration or future extension. It is important to note, this is a proof of concept. While not a finished product, the artefact promises for future development and proves there is a gap for this artefact within UK cyber deterrence and policy making.

## Integration of Risk Modelling and Ethical Guidance

The simulation links quantitative modelling with qualitative judgement. This integration is achieved through:

* Decision trees that trigger specific advice based on input combinations
* Reference material embedded directly into output (Links to NCSC, GDPR etc)
* Colour coded indicators for threat levels and policy sensitivity

This approach ensures users and not just shown numerical scores, but guided towards informed, ethically sound policy decisions.

# Chapter 5: Testing and Evaluation

# Chapter 6: Conclusion and Recommendations

# References

Montasari, R (2023) Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. Countering Cyberterrorism [online]. 101, pp. 7–25.

Ghafur, S., Grass, E., Jennings, N.R. and Darzi, A. (2019) The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health [online]. 1 (1), pp. 10–12. Available from: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30005-6/fulltext>.

Cornish, P. (2021) The Oxford Handbook of Cyber Security Google Books. 2021 [online]. Available from:https://books.google.co.uk/books?hl=en&lr=&id=jIlNEAAAQBAJ&oi=fnd&pg=PT301&dq=offensive+cyber+deterrence+strategies+as+tools+of+conflict+prevention+&ots=lItY21SJzG&sig=ciMJpLOnszd0QXIvcc184ga3v54#v=onepage&q&f=false [Accessed 21 July 2025].

Helkala, K., Cook, J., Lucas, G., Pasquale, F., Reichberg, G. and Syse, H. (2022) AI in Cyber Operations: Ethical and Legal Considerations for End-Users. *Artificial Intelligence and Cybersecurity* [online]. pp. 185–206.

Sexton, M. (2016) U.K. cybersecurity strategy and active cyber defence – issues and risks. *Journal of Cyber Policy* [online]. 1 (2), pp. 222–242.

Chua, Y.T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G. and Hutchings, A. (2019) *Identifying Unintended Harms of Cybersecurity Countermeasures* *IEEE Xplore*. 1 November 2019 [online]. pp. 1–15. Available from: https://ieeexplore.ieee.org/document/9037589 [Accessed 8 September 2021].

Cornish, P. (2016) Deterrence and the Ethics of Cyber Conflict. *Springer eBooks* [online]. 124, pp. 1–16. [Accessed 8 March 2025].