JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2025, tyaf023
https://doi.org/10.1093/cybsec/tyaf023

Research Paper

On human-centred security: a new systems model based on modes and mode transitions

Edwin J. Beggs [1,*], John V. Tucker [1,*], Victoria Wang [2,*]

[1]School of Mathematics and Computer Science, Computational Foundry, Swansea University, Bay Campus, Fabian Way, Swansea SA1 8EN, United Kingdom
[2]Department of Sociology, Zhejiang University. Room 1138, Block A, Creative Building, Zijingang Campus 310058, P.R. China

*Corresponding authors. Edwin J. Beggs and John V. Tucker, School of Mathematics and Computer Science, Computational Foundry, Swansea University, Bay Campus, Fabian Way, Swansea SA1 8EN, United Kingdom. E-mails: e.j.beggs@swansea.ac.uk; j.v.tucker@swansea.ac.uk; VictoriaWang, Department of Sociology, Zhejiang University. Room 1138, Block A, Creative Building, Zijingang Campus ,P.R. China 310058. E-mail: victoriawang99@zju.edu.cn

Received 3 May 2024; revised 25 February 2025; accepted 22 April 2025

Abstract

We propose an abstract conceptual framework for analysing complex security systems using a new notion of *modes* and *mode transitions*. A mode is an independent component of a system with its own objectives, monitoring data, algorithms, and scope and limits. The behaviour of a mode, including its transitions to other modes, is determined by interpretations of the mode's monitoring data in the light of its objectives and capabilities—these interpretations we call *beliefs*. We formalise the conceptual framework mathematically and show how to quantify and visualise beliefs in higher-dimensional geometric spaces. The mathematical models are based on *simplicial complexes*. Our theoretical models are intended to help design, analyse, evaluate and explain systems that provide human-centred services facilitated by software, when confronted by critical security situations, both human and digital.

Keywords: security scenarios; critical incidents; explainable systems; resilience; hierarchical systems; modes; mode transitions; belief functions; simplicial complexes

Introduction

Security, like safety, is defined by a human context. When studying a software system with a specification, its security is more than a matter of the evaluation of its correctness relative to its specification. What it does in human situations, seen and unforeseen, and the possible consequences matter. Thus, ultimately, security is judged outside the technical world of the system and its specification. Developing this point about security further, of importance for security are critical incidents in which harm to people are possible, immanent or current. The security of a system is intimately connected with expectations and assumptions about the wider human-centred systems it serves: *cyber security involves more than cyber*.

Here, we address the question:

How can we accommodate some human aspects of security systems? Can we develop conceptual frameworks and systematic methods for modelling security systems and their operation in a human context?

In seeking some general theory for security, we turn to general system theories and emphasise the role of scenarios in which systems and people relate. General system theory is a loosely defined (huge) portfolio of conceptual frameworks and models for all sorts of complex systems, whose ideas try to capture: how systems are made up of components; how components cooperate; how systems and components perform in their respective environments; and how components can themselves be seen as systems.

Common to all complex systems is the role of data about the behaviour of systems and their environments. Notably, ideas from general system theory are to be found in our everyday language, as well as in our technical methodologies for designing systems, physical, virtual and human.

That 'system thinking' is used widely in so many contexts is worthy of reflection. Its rise is a part of post-war intellectual history [1]. It has profoundly influenced computing, of course, where its focus is on constructing new systems [2]. However, its ubiquity is more

to do with 'systematising' aspects of the world–with de-constructing and re-constructing situations, processes, etc. It is this latter aspect of system thinking that we emphasise here.

Specifically, we offer a new general system model whose central ideas are those of

(i) modes of operation,
(ii) interpretations of monitoring data,
(iii) derived judgements and beliefs about actions to be taken,
(iv) fitness of modes and protocols for changing modes, and
(v) the transparency of these features.

Our new model will be described in three stages. First, we give a set of working definitions and principles that make a theoretical framework for thinking about systems in terms of modes; this is to establish the flexibility and scope of our informal system model and introduce its novel formalisation and geometric visualisation methods.

Secondly, we apply the framework in describing some security situations; these are to explore–and to test–how our ideas can (re)-construct human-centred systems, and to explain by means of examples how modes and mode transitions arise and their data are visualised geometrically.

Finally, there is the mathematical formulation of the informally defined system model and its exemplars: we introduce the mathematical ideas through the examples and so, in Appendix A, we give all the necessary mathematical ideas to define our models in general. The formalisation by mathematical models nail down algebraically the modes and their transitions as these are determined by data about the environment and their interpretation. Further, we show that the general algebraic models can be (i) quantified and (ii) visualised geometrically.

Tools for thinking about security systems

Our systems are a mix of equipment, software tools, and people, the latter organised into teams and also act as individuals. These are bound together and animated by data and communications. Structurally, complex systems are made of modular and hierarchical components that are autonomous, yet are cooperative, adaptable and responsive to situations–especially the individuals, depending upon their degree of professional discretion. Any of these components can–and in practice do–fail in some way. The design and performance of such systems in the real world are not easy to specify, measure, predict or audit.

In security, threats and risks change both in their nature and perceived importance. Significant social and economic disruption can have many causes, such as failures of infrastructures and services, or lack of information. (Extreme weather conditions exemplify such disruptions.) However, our societies are held together by data and software. Thus, cyber failures, and attacks where the objective is to make some software components fail, are always meaningful threats to many aspects of contemporary everyday life, and never far away from national security.

In this paper, we will address system design in human contexts, almost from first principles. We propose an abstract conceptual framework for analysing systems using a new notion of *mode* and *mode transitions*. A mode is an independent active component of the system with its own objectives, monitoring data, algorithms, and scope and limits for action. The behaviour of a mode, including its transitions to other modes, is determined by interpretations of the mode's monitoring data relative to its capabilities and in the light of its objectives. These interpretations of data we will term *beliefs*. Crucially, a mode may no longer be fit for purpose and need to be changed to another mode. A system can be in several modes at once.

We formalise the conceptual framework mathematically and, by visualising the beliefs arising from evaluating a mode's monitoring data in higher-dimensional geometric spaces, we argue our theoretical approach and models may help to explore, design, predict, and explain system behaviour. The various mathematical models are based on mathematical objects called abstract and concrete *simplicial complexes*.

To demonstrate the framework, and further explain the mathematics, we apply our models to three security situations:

(i) triage for a large set of data about individuals in order to classify 'persons of interest';
(ii) mapping the potential causes and effects of a cyber security incident;
(iii) examining a multi-agency response to a critical incident, using the UK Gold-Silver-Bronze command structure.

These types of scenario are commonly associated with Tier 1–high priority–risks in national security audits in the UK [3].

Structure of this paper

This paper has general theoretical aims whose new contributions, and their location, are:

0. To state and explore the problem of developing system models that can accommodate technical and human-centred cybersecurity scenarios.
1. To reflect on scenarios and their part in the security systems specification (Sections 'Human-centred security systems' and 'Concluding remarks').
2. To define general concepts and principles for a conceptual framework to model systems using ideas about modes and mode transitions (Section 'Modes and their visualisation').
3. To create geometric structures to visualise changes of beliefs about the behaviour of systems over time (Section 'Modes and their visualisation').
4. To turn the conceptual framework into a rigorous mathematical theory that enables quantification and evaluation of the reasons and beliefs behind decision making (Section 'Modes and their visualisation' and Appendix A).
5. To apply these general methods in three security scenarios (Illustrative security scenarios, I,II,III).
6. To reflect on possible next steps (Section 'Concluding remarks').

In the matter of 5, we explain the mathematical ideas through examples; the general mathematical definitions of simplicial complex and belief function are given in Appendix A. A general mathematical introduction to modes and their theory is our [4]; there, our early thinking about modes was shaped by modelling autonomous *physical* systems.

We thank the referees for their close reading and comments on earlier drafts of this paper, which have strengthened the arguments and widened their scope.

Human-centred security systems

To begin, we observe that human aspects of security are commonly expressed through scenarios.

Responding to security incidents

Central to security are scenarios for critical incidents against which the security of the system can be explored.

Definition 1.
By a *security scenario* we have in mind (i) a hypothetical situation that involves potential threats and vulnerabilities or (ii) a description of a real-life situation, past or present, that manifested threats and revealed vulnerabilities.

Of particular importance are scenarios containing critical incidents.

Definition 2.
A *critical incident* creates an outcome or consequence that is of significant harm to an individual, community, or business, or to public confidence, broadly interpreted.

Any critical incident arising from a system's operation calls for one or more other systems to respond and contain damage, make repairs and restore operation.

A security scenario should contain information necessary to identify parameters that enable a relevant actor to simulate potential threats effectively, with the aim of being ready to prevent, prepare for, detect and respond to critical security incidents. These scenarios typically belong to security professionals, staff and managers of organisations, and policy makers. Scenario-based research is common in cybersecurity. For example, the major role scenarios play in cybersecurity testbed development, as well as in cybersecurity testing for experimental and educational purposes has been thoroughly discussed in the systematic literature review [5].

Scenarios are themselves classified using ideas about risk, e.g., likelihood, impact and mitigation. For example, the *UK National Security Strategy* [6] is based on the assessment of many security scenarios. In the methodology section, the document comments the "plausible worst-case scenario of each risk was then scored in terms of its likelihood and its potential impact. In order to compare the likelihood of one risk against another and to make relative judgements, these plausible worst-case scenarios were plotted on a matrix..."([6], p. 4).

Critical incidents and the Gold-Silver-Bronze command structure of the UK

In responding to a critical incident, many types of agencies and organisations, with their specialist units and systems, may be called upon to collaborate and cope with an unknown and rapidly unfolding situation. Concepts and working principles, based on experience, are needed for this to work effectively. Such frameworks must 'cage the incident' in order to initialise and develop a response; they must also be known and understood by the participating agencies and organisations. In the UK, such frameworks for a diverse set of government agencies and services have been created, used and exercised for decades. To pick one example, relevant to a later case study (in Section 'Illustrative security scenarios III: Critical incidents and gold-silver-bronze command structures'), a glimpse of these frameworks can be found in the Home Office's *Critical incident management for staff of Border Force, Immigration Enforcement and UK Visas and Immigration* [7].

In the UK, the *Gold-Silver-Bronze (GSB) command structure* is used for major operations by the emergency services [7]. The structure was originally created by the Metropolitan Police Service, as a direct response to the Broadwater Farm Riot on the 6 October 1985 [8]. Assessing their responses during this riot, the Metropolitan Police came to the realisation that their traditional rank-based command system was inappropriate and inefficient in dealing with sudden events. (Particularly, on the night of the riot, it was not clear who was actually in charge of the actual operational procedures of the police.)

Thus, the GSB is an informally described role-based system architecture that assigns three different levels of command according to skill, expertise, location and competency.[1] The three levels are *strategic*, *tactical* and *operational command structures*.

Briefly, the Gold Commander is responsible for the strategic direction and has overall control of the distinct resources at the incident. Instead of on site, the Gold Commander is in a distant control room formulating the strategy for dealing with the incident.

Silver Commanders are the seniors in charge of their own organisation's resources that are available at the scene. They are responsible for the tactical coordination, deciding on how to use their resources to achieve the strategic aims of the Gold Commander. Like the Gold Commander, they are also not directly involved in dealing with an incident itself. At the scene of the incident, they will work closely with the Silver Commanders of other organisations, operating from a purpose-built command vehicle or makeshift command room(s), known as the Joint Emergency Services Control Centre (JESCC).

The Bronze Commanders are responsible for the operational implementation, directly controlling the resources of their organisations and working with colleagues at the scene of the incident. Bronze Commanders may share responsibilities and tasks in complex incidents and assume responsibility for different areas, if an incident is widespread geographically.

During the initial stages of an incident, the first member of the first organisation to arrive at the incident temporarily assumes the role of Silver or Bronze Commander until relieved by a more senior member of their organisation. It is noteworthy that these three roles are not restricted to ranks, though invariably the chain of command will follow the order of rank.

Although the GSB command structure was originally devised to respond to sudden major incidents, it spread-out in all police forces and emergency services, and has been frequently used in pre-planned operations (e.g., the policing of football matches or firearms operations (cf. [7])).

On deploying a GSB command structure for a critical incident, we have a human-centred hierarchical system that must adapt to complex events–and to what may or may not be known about them–that is dependent on data and software from multiple sites and sources.

Modes and their visualisation

Modes decompose and categorise the various objectives and behaviours of a system. A mode collects relevant data and applies algorithms to govern the behaviour and external communication.

What is a mode?

Here is a working definition to begin building the conceptual framework:

Definition 3.

1 In some cases, the national government (via the Cabinet Office Briefing Rooms) assume ultimate control and act as a fourth, platinum level (Home Office, 2021).

Consider a system S operating in an environment E. A *mode* of the system S is defined by these characteristics:

(1) A mode is associated to, or determines, a subset of the possible states of the system.
(2) A mode is designed to deliver on certain objectives for the system when in these states.
(3) A mode consists of
  (a) methods to input data from the environment E and to output data to E
  (b) data types and algorithms for implementing the objectives.
(4) A mode has means to evaluate its performance against its objectives and, if necessary, choose and transfer to another mode.

Thus, a mode is responsible for specific aspects of the system's performance. A mode's purpose may be expressed in its narrowly defined technical objectives, or in some high-level objectives expressing the primary purposes of the whole system. A mode may act autonomously, or be a hub for accessing other modes, or be a unit of people with expertise. Each mode owns its relationship with the environment according to its objectives. We choose the term 'objectives' to suit the great variety of scenarios we have in mind for our development of system models.

Principles for designing modes

With the initial intuitions of Definition 3 in mind, we can formulate some design principles to develop a conceptual framework for thinking about systems in terms of modes and mode transitions.

Completeness. A set of modes for a system is a classification of the operation or behaviour of a system. At any time, a system can be in one, or more, modes.

Composition. When a system is in a number of modes then that situation itself constitutes a mode.

Component. A set of modes for a system consists of (i) a set of *basic modes* and (ii) *joint modes* made by combining modes.

Localisation. Each mode possesses its own data to monitor its behaviour and environment. This monitoring data determines a local state space called the *evidence space* of the mode that represents what its modes can know.

Thus, knowledge of the system at any time is localised to the modes at that time.

Globalisation. What the system can know about its environment is a synthesis of what its modes can know of the environment through their monitoring data. By combining the evidence spaces, an idealised global state space for the system is possible for reasoning.

Quantification. If a state of the system is meaningful for a number of modes then the relevance or suitability of these modes for the state of the system must be quantified, calibrated and interpreted.

Visualisation. With quantification and calibration comes the possibility of visualisation via geometric objects drawn to scale and via derived qualitative diagrams.

Shortly, we will show how to visualise in space the basic modes by vertices, and the joint modes arising by combining them as lines, triangles, tetrahedra etc. The geometric objects we build in this way are called *simplicial complexes*. Simplicial complexes are made up of geometric pieces called *faces*. The evolution of the system in time is given by a path through the geometric simplicial complex, making obvious which mode the system is in at a particular time; indeed its exact positions can indicate something of its past, present and possible futures.

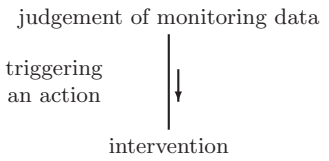

Figure 1. Visualising a mode transition for a trigger mechanism.

Modes and faces. In a successful system model using modes, *every face of its simplicial complex is a mode and every mode is represented by a face*.

Quantification can take the form of a position in the space representing the suitability of the mode for the state of the system, in a line or triangle or tetrahedron, etc. representing the joint mode.

Belief. The position on a face is computed by *belief functions* that from a state of the system calculates a measure of the relevance to that state of the modes of the face.

In the time evolution of the system we need to decide

(i) if, and when, a system should change from one mode to another, and
(ii) which new mode should be chosen.

Thresholds. The transition out of one mode into another is governed by the results of the quantification and calibration. The decision to move to a new mode may be specified by numerical thresholds. Transition has these stages:

(a) the realisation that the mode is approaching its limitations
(b) the selection of modes that could be more appropriate
(c) triggers to choose and change to a new mode.

The belief functions, in computing relevance, are a means to trigger changes of mode.

Explanation. The conceptual system of modes, belief functions, mode evaluation, thresholds and mode transition functions, and their visual representation in simplicial complexes, can serve as an explanatory framework for the dynamical behaviour of automatic systems.

In particular, the position and path over time (the trajectory) in the simplicial complex visualises the dynamics of decision making by the system.

Simple security examples

We consider some simple examples to begin to shape our informal ideas of a system of modes, the evaluation of beliefs and how they might be visualised.

Example 1 (A simple trigger).

Fig. 1 represents visually a trigger for action that has three modes: two vertices and one line. Consider the line between a mode that makes judgements of some attribute using data from monitoring the environment (the point at the top of the interval) and the mode that performs an intervention (the point at the bottom). Unlike a usual state transition graph, where lines merely represent transitions or jumps, here the line *itself* represents a mode where the decision to intervene unfolds according to its monitoring data. These observations are formed into a numerical quantification of beliefs about the state of the system and visualised as points along the line, beginning at the top and moving to the bottom. Threshold points on the line begin to warn, and then trigger, a change of mode; on reaching the bottom, the intervention begins.

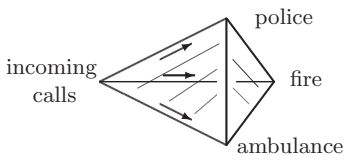

Figure 2. Visualising a triage for emergency services.

A witness can note the position along the line to see how things were going, and perhaps be reassured that the course of action was progressing correctly. Such a point on a line indicator is quite a common visualisation (e.g., as with a progress bar that simply estimates time taken for a task to be completed). Here, however, the line indicator is displaying an interpretation of information which the control system is actually using to make decisions. If the point is near the top, then a witness knows that the control system has no intention of intervening because they are looking directly at the system's own assessment of the situation. □

In this first example, we see that a key to the transparency of decision making is continuity. We do not discontinuously move between vertices on a graph, but have a continuous motion in a geometric visualisation, which allows *an estimate of what the system is about to do and when*. Without continuity we have a system whose behaviour could change drastically and unpredictably. Of course, there might be a good reason for this, but, for safety and reliability, predictability is an important consideration. We make a general comparison between visualising system change using complexes versus graphs in Appendix A, Section 'Simplicial complexes and graphs'.

Of course, a key to transparency is reliability, that what we see is really related to the state of the system. This means that *the geometry of the visualisation must be intimately related to how the system actually makes decisions*.

Example 2 (A simple emergency).
In Fig. 2, we consider a notification that warns of a possible incident–such as personal attack, social disturbance, or collision of vehicles. In general, the incident could involve some or all of the primary first responders of police, fire brigade and ambulance. These are represented by vertices in the diagram. As more information becomes available over a (hopefully short) time period, relevant choices of services can be made and deployed to the scene. In particular, between the separate actions of, say, deploying police and ambulance we have a combined action of doing both simultaneously, and that is represented in the diagram by a line between the two vertices.

Altogether the 15 faces of the diagram in Fig. 2 represent 15 modes of the system. The filled-in tetrahedron between the four vertices is the mode which gathers all available information and assesses the response. When beliefs about the state of the system (represented by a point in this tetrahedron or 3-simplex) reaches the triangle at the end, then full deployment is instigated. If the incident in some way is misrepresented then the point moves, possibly returning to the warning vertex, and then to the rest of the system (not shown). When an action is actually taken it should be a combination of the three action services (vertices), depending on where the point is in the rightmost triangle. □

Geometric intuitions

Systems frequently have to take account of several factors or carry out several tasks, and we can take account of this by allowing combinations of modes to also form modes–the joint modes of Section 'Principles for designing modes'. If basic modes are vertices, these joint modes translate into edges, triangles, tetrahedra, etc. In general, we shall represent beliefs about the state of a system as a point in a face of a simplicial complex. What exactly is a simplicial complex?

A 0-simplex is just a point, and a 1-simplex is a line between some of the 0-simplices. Thus, a simplicial complex consisting of only 0 and 1-simplicies is just a graph whose edges are the 1-simplices and whose vertices are the 0-simplices. We shall not assume that this graph is directed: if there are arrows they are either imposed by principles (e.g., not being able to stop an intervention once triggered) or by the current objectives. Increasing the dimension, a 2-simplex is a filled-in triangle and a 3-simplex is a solid tetrahedron, and so on. Fully general definitions are given in Appendix A. A point to remember is that *simplicial complexes generalise planar graphs*.

Consider the visualisation of the simple emergency with its 15 faces in Fig. 2: there are four 0-simplicies, six 1-simplicies, four 2-simplicies, and one 3-simplex. Each of these is a mode.

The belief about the state of the system is visualised as a point in the geometric simplicial object; the position in a face shows which modes the system is in and which mode is likely to come next. The position is given by the belief generated by algorithms on the basis of evidence. Technically, there is mathematical belief theory that is a generalisation of probability theory and, again, we refer to Appendix A for a more formal discussion.

As the modes are linked to the behaviour of the system, the visualisation of the modes gives the current behaviour of the system, at least its intentions and its capabilities.

Illustrative security scenarios I: triage and persons of interest

We now apply these ideas to three examples. We describe the first in some detail, including its mathematics; the others are less detailed due to their more open-ended nature and limitations of space.

Scenario

Consider persons coming to the attention of the police as potential security risks through an initial assessment process or triage. We will explore this scenario by describing a system of modes whose function is to perform the classification.

State space and design

In the design process we first start with our 'state space', which will be the set of people in a country, together with their recorded actions and beliefs. To be more exact, we take a cover of the set of 'people of interest' in the population. We wish to classify those into the following subsets:

PeopleofInterest (PoI) – those who have come to the attention of the security services
BeginTriage – those who are in process of classification by the triage process
Opportunity – those who are in a position to cause damage by, e.g., access to public platforms or proximity to high value targets.
Concern – those who have extreme views or contacts which could pose a security concern.
SecurityClearance – those who have been granted clearance for certain activities
FurtherInvestigation – those who are under active investigation by the security services

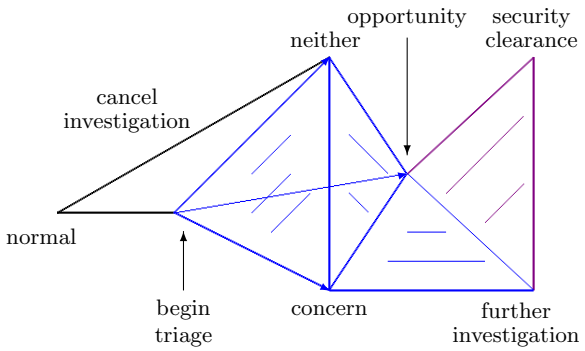

Figure 3. Initial assessment for potential security risks.

These and other subsets of the population are assigned as state spaces for basic modes. It is clear that a person may be in several of these subsets, whence they belong to joint modes. For example, an individual who is in both *Opportunity* and *Concern* is a larger threat than a person who is in just one of the subsets.

Now, we consider how to determine whether a person is actually in one of these subsets. This could include examining criminal or financial records or interrogation. This process results in a *space of evidence*, and using this we calculate the belief functions which we use to choose which subsets we believe a person belongs to. These beliefs are continually updated as, e.g., an investigation comes to an end or new evidence is presented. The belief functions can then trigger a change of mode, e.g., moving to a security clearance process. Of course, the computed belief functions are only an approximation of the true state of affairs, as any process is error prone.

Scenario and its visualisation

Our scenario is sufficiently simple to be described directly using modes and their geometric representation: consider Fig. 3. We begin at the 'begin triage' vertex of the blue tetrahedral mode 'triage'. After conducting an initial investigation, 'triage' outputs either (i) a value along the edge from 'opportunity' (i.e., there is an opportunity to carry out an attack, e.g., the subject is in close proximity to potential targets) to 'concern' (i.e., there is evidence that the subject may be a security risk), or (ii) the vertex 'neither' of the above.

From 'neither' the investigation is cancelled, possibly deleting material as procedures allow. From the vertex 'opportunity' on the edge (i.e., there is minimal concern about a security risk), the purple triangle 'obtain security clearance' mode is started. This will get references from contacts of the subject, etc. From anywhere else on the edge (i.e., there is *some* concern about security risk), the red 'consider further investigation' mode is entered. It is possible to move between the 'obtain security clearance' and 'consider further investigation' modes if new evidence is uncovered. The end points are either being granted 'security clearance' or being entered for a full 'further investigation'. To repeat, there are four outcomes and we can leave the triage mode at three vertices or *at one edge*.

Inspecting the diagram, there are 7 0-simplices, 12 1-simplices, 7 2-simplices, and 1 3-simplex. Thus, the model reveals that there are, in principle, 27 modes in this scenario.

Quantification: space of evidence and thresholds.

The above informal description is now quantified and modelled mathematically. We will build a relevant belief function to plot points based on the evidence available; these points lie in the blue triage tetrahedron.

First, we must mathematically model the space of evidence. This will be based upon concern and opportunity. We begin with choosing positive numbers

$$(x_{\text{begin}}, x_{\text{con}}, x_{\text{opp}}).$$

These numbers are ratios having the general form of

$$\frac{\text{individual score}}{\text{preset score}}.$$

In this case the numbers try to measure concern x_{con} and opportunity x_{opp}, and they are estimated as follows.

We take $x_{\text{con}} \geq 0$ to be a weighted sum of evidence from phone calls, emails and social media posts etc., divided by a preset 'level of concern' and capped at 1; so $x_{\text{con}} = 1$ is taken to be a significant concern and $x_{\text{con}} = 0$ is no concern.

We set x_{opp} to be a sum of events attended by the person, weighted by the profile of the event or ease of attack, again divided by a preset level and capped at 1; so $x_{\text{opp}} = 1$ is taken to be a significant opportunity. For instance, a large number of applications to certain events would also be treated as a cause for concern, so these numbers are not independent.

We might assign $x_{\text{begin}} \in [0, 1]$ as the fraction of the checks remaining to be made; so if we had 54 checks in total to perform we would begin at $54/54 = 1$ and then count down as checking tasks were completed. However, we may cut short the process if we already have enough evidence to escalate the investigation. We now define

$$x_{\text{end}} = \max\{1 - x_{\text{begin}}, x_{\text{con}}, x_{\text{opp}}\}.$$

Our space of evidence is this cube of triples:

$$(x_{\text{con}}, x_{\text{opp}}, x_{\text{end}}) \in [0, 1]^3.$$

Consider Fig. 4, where the origin O is the most distant vertex from our point of view. We highlight the subsets of evidence where we believe that the four outcomes are true.

Thus, in the second diagram in Fig. 4 in the red subset we have points in the neighbourhood of the region where $x_{\text{con}} = 1$, i.e., where we believe that we should be at the vertex *concern*.

In the third diagram in Fig. 4 in the blue subset we have points in the neighbourhood of the region where $x_{\text{opp}} = 1$, i.e., where we believe that we should be at the vertex *opportunity*, and similarly for the leftmost diagram and the vertex *opportunity*. The vertex *begin* has a subset on the right given by a cube $[0, 1 - \epsilon)^3$ for some small $\epsilon > 0$.

Quantification: belief and visualisation

To define the function that visualises belief, we now construct a partition of unity for the cube $[0, 1]^3$ (as in Definition 12 in Appendix A) for the above subsets. The subsets for *opportunity* and *concern* intersect as we can have an output along the edge linking those vertices. However, we do not allow the subset for *end* intersect subsets for *opportunity* and *concern*. as those are not valid outputs on Fig. 3. This is because making discrete decisions from continuous data requires some amount of discontinuity–made easier in our case as our data are actually rational numbers. Part of the choice of belief function is minimising the likelihood of discontinuity to make the system as transparent in real time (i.e., as predictable in the short term) as possible.

Mode objectives

Each mode can be assigned objectives. For example, the mode defining the rightmost triangle in Fig. 3 has an objective which is to grant

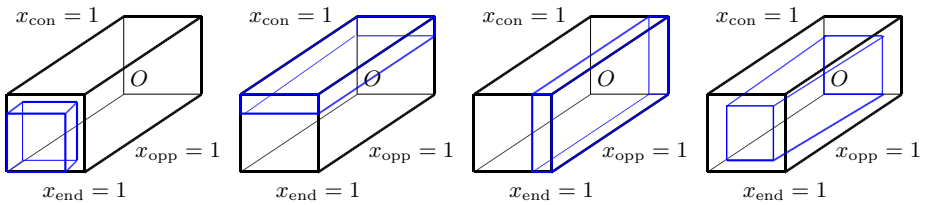

Figure 4. The subsets for neither, concern, opportunity and begin respectively.

security clearance if possible, and if not refer the subject for further investigation. The objectives of the system are achieved by being distributed among the objectives for the modes.

Illustrative security scenarios II: cyber architectures and ecosystems

In responding to a cyber attack on a component of a software system, a range of concerns arise for the system architecture and its ecosystem, *viz.* other components of the system, the external services the system depends upon and delivers, and the external systems it serves. Commonly, some of these dependencies may be unclear or unknown. We will express some of the issues that arise in terms of modes.

Malware

Systems can be viewed at high level (simpler, hopefully transparent) and low level (complicated, likely opaque, due to lots of legacy code and platform dependencies). A problem is decisions made at a low level, e.g., using a buffer overflow to change the status of a block of code from non-executable to executable. This occurred in EternalBlue, the exploit behind the WannaCry ransomware cyber attack of 2017, which affected National Health Service (NHS) hospitals in the UK. One reason why some NHS systems were vulnerable to WannaCry was the problem of upgrading systems which have to be online continuously. The WannaCry worm bulk encrypted data on the affected machines, so systems which had reliable backups were less affected. The WannaCry cyber attack was effectively halted by the activation of a built in kill-switch by registering an external web site, a method detected and implemented by an individual about 7 hours after the attack began. Though quick enough to stop much more damage being caused by WannaCry, such a timescale may not be much use against a more malicious attack, e.g., data theft, timed disruption of vital services or physical damage to critical infrastructure. Such an attack could use security flaws not used before.

Human intervention takes time, and counter-measures may be difficult to circulate as some communication systems may have been affected or taken out by the attack. The first line of response is the isolation of critical systems as much as possible. This requires designs with inherent resistance to attack defined by scenarios and associated exercises to prepare for responses.

As with a pandemic, an obvious line to take is compartmentalisation–isolating things from each other to make spread difficult by not sharing resources. How do these observations relate to our concept of describing a system of in terms of modes? What security features can be designed for such systems?

Maintainence: runtime updates and shadow modes

Consider the idea that modes can be 'shadowed' by duplicate modes, whose job is to have the same data and operations as the original

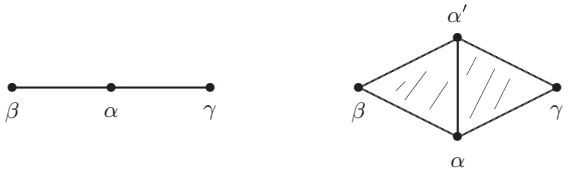

Figure 5. Adding a shadow mode α'.

mode. If an original mode needs to be taken offline (e.g., for upgrade) then the shadow mode can be switched into its place. A shadow mode could also operate under a time delay or with different security options from the original mode, making it less likely to be compromised in an attack than the original mode (but at the cost of not having quite the same data).

Symbolically, let us start with a simple system with three basic modes, such as $\mathcal{M} = \{\alpha, \beta, \gamma\}$. We now add a 'shadow' mode α' for α, giving four modes $\mathcal{M}' = \{\alpha, \alpha', \beta, \gamma\}$, as in Fig. 5. When the shadow mode is activated the effect is to copy all modes containing α – in Fig. 5 we have copies

$$\{\alpha'\}, \{\alpha', \beta\}, \{\alpha', \gamma\}$$

of modes $\{\alpha\}$, $\{\alpha, \beta\}$, $\{\alpha, \gamma\}$, respectively; and we also have new modes

$$\{\alpha, \alpha'\}, \{\alpha, \alpha', \beta\}, \{\alpha, \alpha', \gamma\}$$

that link the shadow and original modes.

When the shadow is set up its first task for the linking modes (say for $\{\alpha, \alpha', \beta\}$) is to copy the state and data for $\{\alpha, \beta\}$ to $\{\alpha', \beta\}$. It will continue to maintain the shadow copy $\{\alpha', \beta\}$ up to date, but all actual decisions will be taken by the dominant copy $\{\alpha, \beta\}$. The log for $\{\alpha', \beta\}$ will be kept for comparison to determine if there is any significant difference between the copies. (This could be as a result of a hardware problem or one of the copies being compromised.) At some point the roles of the shadow and dominant copy can be reversed, and then the new shadow copy can be shut down and updated or repaired.

The cost of the approach

Shadow modes are proposed only for critical systems, not systems which can afford to be offline for the time that conventional backups require (although this could be weeks or months if proper preparation was not made).

The proposed system of shadow modes is expensive in terms of the size of the system, but the locality of the mode structure puts an upper limit on how many shadow modes are required. The requirements would be linear in the total size of the system times a higher degree factor of the local complexity, involving how many simplexes intersect at a vertex.

Compartmentalisation of function

Modes are assigned according to function, and are given only the tools (file access, external links, etc.) that are needed to perform that function. Regarding WannaCry, the options to bulk delete or encrypt data would simply not be available in most modes. It is not a matter of rewriting their code, the options to do that would not be on their allowed list of operations or they would not have the codes to access those options. They would not even know where to go to be able to access those codes.

A malicious worm would likely have to be able to go through several modes and their isolation mechanisms before it was in a position to cause harm. It is this movement at the high level of the modes is just what transparency and visualisation of the mode diagram is designed to detect, whether by a human or an AI supervisor who could then shut down the system or take other measures.

Isolation of modes

Different modes do not share software with each other. At the design stage methods or classes may be inherited based on inclusion of modes–i.e., mode $\{\alpha, \beta\}$ may inherit from $\{\alpha\}$. However these will be compiled into distinct copies in memory, so there is no common memory at runtime. Thus, if one mode is corrupted the other modes will be unaffected unless a virus manages to propagate from mode to mode or send corrupted data. This forms a bottleneck in the infection process which can be examined in more detail. When an alarm is raised communication between modes may be further restricted.

External monitoring of modes

As operations on any external system (e.g., databases) are performed by oracle calls from the modes, the number of uses of such calls can be logged by a system not connected to the current operating mode, and an alarm raised if usage exceeds a prescribed amount. Flagging a mode as potentially compromised could restrict the oracle calls it would make, effectively cutting it off from secure databases, etc.

Attack trees

Consider attack trees and cybersecurity (see, e.g., [9]). The tree displays the steps needed for a successful attack, with nodes being tagged logically with 'or' or 'and'. They have been generalised to attack graphs in [10]. With simplicial complexes generalising graphs, attack trees can be related to the mode approach and generalised by simplicial complexes.

As with the original paper on attack trees [11], we consider an attack to obtain unauthorised access. In Fig. 6 is an attack tree for accessing a system (not detailed and not necessarily accurate), including combining causes with 'or' and 'and'. One way is to take control of a computer which is logged into the system. Alternatively, we require some combination (likely all three of) userid, password and phone number. In an attack tree these would be nodes joined by 'and'. Instead, we are more general than that by combining these causes by a tetrahedron, which allows for more complicated dependences, e.g., there might be ways to obtain two factors simultaneously, or only two out of three might be needed in certain circumstances.

In effect, we are describing a simplicial mode structure of a system whose purpose is to attack another system. In a scenario, each event in the attack tree takes place in a mode, and placing the events gives a generalised simplicial map from the attack tree to the simplicial complex of modes. Generalised, as the thick lines in Fig. 6 may be divided into several lines, indicating that the system may pass through several modes before reaching 'obtain access '. Modelling different scenarios would include considering different simplicial maps.

For example, a sleeping worm might have been placed in a system, but whether it is discovered prior to activation could depend on the actions taken by the system in the meantime. An attack tree might have an event which is easier in certain modes of operation.

Using simplicial maps, we could exploit the geometric formulation of mode-based systems and attack trees to automate the checking to what extent a given system is resistant to a given form of attack.

Cyber resilience

In theorising our new system model we are exploring and making precise a range of security scenarios that combine physical and human actions, and in which collecting, computing, communicating and interpreting data are fundamental. We are not focussed on cybersecurity *per se*. However, the mode system model has certain strong points concerning *cyber resilience*. Put simply, resilience is commonly taken to mean the ability of a system to continue with some level of service, to be repairable and to return providing its normal services in good time. Thus, cyber resilience highlights the domain and the software in thinking about the system. To quote the introduction to NIST's *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, [12], p.1:

'Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.'

Like explainability, resiliency is a factor for trust in a system that involves the domain in which the software finds itself.

Some of the strong points mentioned above are these:

(1) *Tools for system thinking*. Our 'whole-system' approach is intended to map and model interactions between people, equipment and computer systems, and the environments they find themselves in. This is not easy. We are posing the problem of using general system-based thinking and mathematical models to analyse such complex (necessarily human-focussed) systems. Further, we offer a *prima facie* case that this is possible with our modes model.

(2) *Transitions*. Our model highlights the interpretation of data and its connections with objectives and decisions. Interpretation is quantified by our so-called belief functions and the paths traced in simplicial complexes measuring the system's behaviour and its relationship with modes. The quantified interpretations of data enables the highlighting of processes of (i) checking a mode is 'fit for purpose' and (ii) triggering change to a potentially more useful mode.

(3) *Interdependence*. Our model can address the resilience of systems via analysing their compartmentalisation and refactorisation in terms of modes.

Transitions are central to resilience as they are the response to disrupting events. Routinely, they are needed in security screening and the practical problem of deciding the presence or absence or likelihood of 'malware'. Now, the common form of representing transitions are planar graphs, which may or may not have weights or probabilities attached. Simplicial complexes are a compact, higher-dimensional, continuous geometric generalisation of planar graphs. The continuity and geometry can offer actors in a component failure event some form of information, and possibly automation.

The modes system model can address attacks on more than one system and their dependencies. For example, this is relevant in industrial situations where there are enterprise software and operational software. The enterprise systems of a factory will likely benefit from well-established technical support; the operational systems will likely

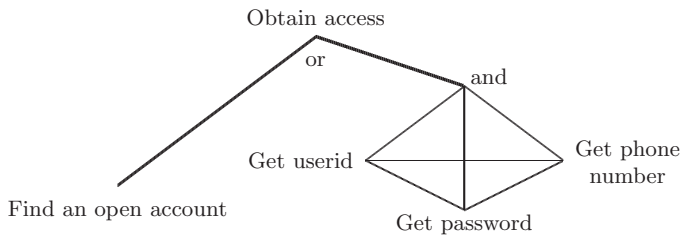

Figure 6. An attack 'tree' for unauthorised access.

be bespoke and more vulnerable–see, for example, the informative resilience case study [13]. It may be that operational resilience is more important financially than enterprise. Multiple attacks are likely to occur at the beginning of a major conflict especially on critical infrastructure. However, critical infrastructure is notoriously difficult to conceptualise and theorise [14]. Given that some zero-day exploits are likely to be used in a major (state sponsored) cyberattack, clearly resilience is a critical and underdeveloped area for research.

A system delivering physical world services is enabled and sustained by computer systems, and its resilience requires a portfolio of scenarios including not just breaches of cybersecurity and software failure, but also the effects on the services for which the software exists. It seems to us that there is a gap in concepts, models and tools for dealing with security scenarios in which software systems are a key enabling component for activities involving equipment and people, both as actors and users.

Illustrative security scenarios III: Critical incidents and gold-silver-bronze command structures

Various scenarios are involved in preparing plans for responding to critical incidents, which should be able to generate simulations. In a multi-agency response to a critical incident, streams of decisions need to be made by different commands drawing on different streams of information about an unfolding situation. However, this can easily lead to confusion and information overload as hundreds of pieces of information, many inaccurate, flood in. Triaging, compiling and interpreting this information to formulate beliefs about the situation and to suggest a number of options are necessary tasks; how could these be supported or partially automated? We examine the general form of the gold-silver-bronze command structure, introduced in Section 'Critical incidents and the Gold-Silver-Bronze command structure of the UK', though a toy example of a critical incident. These structures are likely to be broadly similar in many incidents.

Scenario

Consider an event where a bomb has been detonated in a football stadium during a game.

Our first point of view is that of taking control of the incident. In general, after an emergency 999 call, one of the emergency services (police, ambulance, fire) will attend. But in our case, police will be on site and will radio their control to declare a 'major incident', thus initiating the *gold-silver-bronze command structure*.

In our scenario, all three services are on site. Each of the services will set up their own silver command structures who will be in operational charge of the incident and will be located on or close to the incident. In our case, it is likely that a police inspector or superintendent would be at the match and would take this position. The fire and ambulance services should also have their silver commander on site, and preferably all the silver commanders would gather at the same place to allow free communication. A separate communications channel will likely be cleared for the incident.[2]

The bronze commanders for each of the services will be in charge of various physical locations in the incident, and will report to their silver commander. The number and deployment of the bronze commanders will vary greatly and depend on the nature of the incident.

The gold command is the top-level strategic post, which establishes strategy for the combined operation, gathers and allocates resources and liaises with government, and other organisations and agencies.

Modelling belief

Fig. 7 shows the modes for setting up the silver command, building on the triage example earlier (Fig. 2). The usual command structure is the police-fire-ambulance triangle, and this changes to silver command on a declaration of a major incident. We have shown an algebraic product of a triangle with an interval as a cylinder in the figure, but in fact the modes are rather more complicated. This would allow for delays in setting up some of the silver commands (real incidents are often chaotic).

Fig. 7 also shows the gold structure, based on coordination of the three services, and their links to the media, politicians (for resources) and local councils (for facilities such as shelter).

In principle, one bronze commander is assigned to each physical area of the site and is in personal command of the teams there. Fig. 8 depicts the geographical layout of the areas in the stadium scenario, with the positions of teams indicated (the local stadium security coming under police command). Each area should have a bronze commander, who reports to the appropriate silver commander, and then communicates with the teams in the area.

Concluding remarks

Reflections

Given the questions posed in the introduction, a general aim is to develop rigorous methods and mathematical models for thinking about current and new systems in complex human contexts, described by security scenarios. We believe our work draws attention to some gaps among theories addressing security; perhaps, these arise from a common reliance on loose and implicit assumptions about 'systems'. Thus, 'system thinking' needs strengthening with

(a) precise, informal conceptions of systems that shed light on a wide spectrum of security situations
(b) tools for structuring and analysing scenarios for specifying, testing and evaluating designs of systems

2 If the military (other than explosive experts) become involved they may take overall charge.

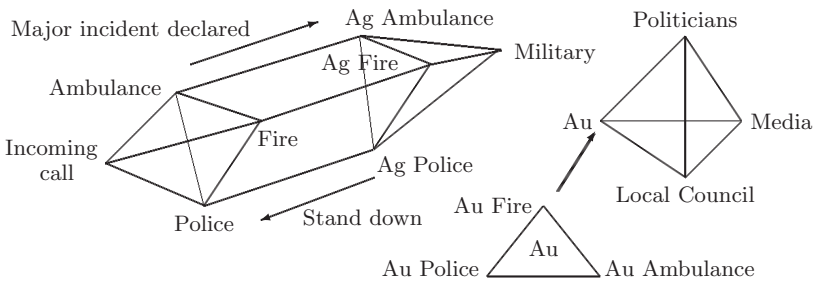

Figure 7. The silver (Ag) and gold (Au) command structures.

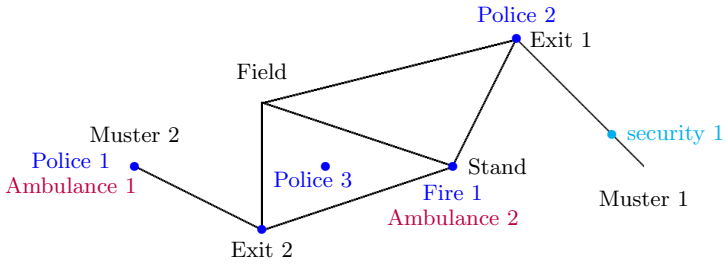

Figure 8. Bronze command and the geographical layout of teams.

(c) tools to map and integrate software systems with the human situation in which they are critical
(d) mathematical tools for modelling systems and their environment that can quantify, visualise and help make transparent decisions in security situations
(e) model hierarchical decomposition of systems to approximate to the level of individuals in a human-centred security situation.

These desiderata are relevant to theorising resilience. They can be addressed by further developing our system thinking based on notions of mode and mode transition, which seem to have some advantages, such as the features:

Concurrency: Several modes can be designed to work collaboratively on the same problems.
Independence: The independent modes are designed so as to avoid, or at least contain, potential damage, and to facilitate auditing.
Continuity: Changes can be made to modes separately allowing updates without system downtime. If a mode is behaving suspiciously, this should be recognised by the other modes, and the errant mode could be suspended. If one mode is down, others need not be compromised.
Transparency: The geometric visualisation supports analysis, transparency and explication.

As automation expands into new areas of life through AI, transparency is particularly important and timely.

Next steps

In terms of next steps, there is more to explore in the types of examples discussed in this paper; for example, triage is a hugely important topic, one associated with machine learning. Only through case studies, including realistic applications and the reconstruction of actual past events, can we establish the evidence and so the extent to which the *prima facie* advantages–such as concurrency, independence, continuity, and transparency–actually obtain.

Systems are hierarchical. By drilling down into the internals of the modes, and the mathematics of their geometries and belief functions, we can develop a mathematical theory of modes and mode transitions with a hierarchy of levels.

In the matter of resilience, it would be fruitful to look at the extension of the Gold/Silver/Bronze command model, e.g., to technical scenarios involving cyber attacks. A large scale attack is likely to cause serious disruption to communications as well as other services. A structure to integrate a number of unpredictable human resources at short notice would be required to have any chance of a rapid recovery. This is one of the National Cyber Security Centre's suggestions for 'proportionate and effective governance' [15]. By using the modes-based system structure, we would like to see if this could also be applied to models based on intelligent agents or other software assets.

In due course, we will need to develop specifications for software tools to strengthen the methods and enable simulation.

Theorising scenarios

Setting aside dictionary definitions, the term 'scenario' suggests an idealisation that postulates a context and events that are abstracted from the real world.[3] The term security scenario suggests an account or synopsis of a possible unfolding of events and courses of (re-)action in which local or national security is implicated. Such idealisations are needed for planning responses to security problems; they also shape evaluations, feedback and investigations of historical incidents. Indeed, our understanding of past security problems play an essential role in preparations for future security problems. The same is true of history in military planning and training, of course.

3 Interestingly, the 1982 Supplement to the Oxford English Dictionary remarked "The over-use of this word in various loose senses has attracted frequent hostile comment".

It is plausible to argue that, ultimately, scenarios are both the *raison d'être* for systems as well as formidable tests for their evaluation–their nemesis in security terms. So we might ask:

What is the essential structure of a scenario? Can we develop a rigorous framework within which systems and scenarios can be compared? Can such a framework be formalised?

Over the past two decades, scenarios have also been used as a tool to deal with the complexities and uncertainties associated with global issues, such as climate change, food security, and land use. This allows the simulation of different environments, approaches and outcomes, as well as delivering a multitude of perspectives on potential future developments. Thus, scenario-based research has been frequently conducted by all sorts of professionals.

(To give a sample of fields: economics and business studies (e.g., [16]); political science and international relations (e.g., [17]); environmental science and climate studies (e.g., [18]); public health and epidemiology (e.g., [19]); urban planning and architecture (e.g., [20]); psychology and sociology (e.g., [21]); military war-gaming (e.g., [22])).

One commonly mentioned general description is: "plausible and often simplified descriptions of how the future may develop based on a coherent and internally consistent set of assumptions on key driving forces and relationships" [23]. The set of assumptions are key to the construction of scenarios and their varied application.

Looking ahead at what may count as threats (say, over a decade) suggests to us that new tools and methodologies for thinking about security scenarios, idealised and actual, should be useful and are, in fact, needed. Scenarios play an essential role in creating security systems, in assessing risk more broadly and judging their resilience.

Making a stocktake of technologies that we know currently and which may come to some sort of maturity in the coming decade is an interesting exercise (e.g., [24]). Every new technology can generate new surprises for security, broadly conceived. Security surprises can also come from ill-understood functional interdependencies of: current systems, or mutually dependent sets of users, or underlying, shared computing infrastructures. Most importantly, we note that *our surprise may be proportional to our ignorance of these factors and their effects*. If the critical technologies of the next decade are unknown then security surprises are classic 'unknown unknowns'. Thus, to avoid, or at least partially prepare, for surprises we may turn to scenarios.

We believe it sensible to seek new theories about security scenarios that abstract from lived and imagined experiences and, specifically, seek rigorous, systematic and useable methodologies, some mathematical models, and software tools. In particular, they must make explicit the various roles that data and automation play in decisions by the systems involved.

Author contributions

Edwin J. Beggs (Conceptualization, Formal analysis, Methodology), John V. Tuckery (Conceptualization, Formal analysis, Methodology), and Victoria Wang (Conceptualization, Formal analysis, Methodology).

Conflict of interest: None declared.

Funding

The authors would like to acknowledge the support by UK's Accelerated Capability Environment ACE-C391 National Security Tech Surprise.

Appendix A: The mathematics

A.1. Logical and geometric methods

In Definition 3 a mode is described in terms of subsets of the states and objectives of a system. The mathematics of how to deal with a set built as a union of subsets has been known for a long time–a simplicial complex [25].

Definition 4.
An *abstract simplicial complex* $(\mathcal{M}, \mathcal{C})$ is a collection $\mathcal{C}$ of finite subsets of a set $\mathcal{M}$ such that if $Y \subset X$ and $X \in \mathcal{C}$ then $Y \in \mathcal{C}$.

Definition 5.
A collection of subsets $U_\alpha \subset S$ (for α in some index set $\mathcal{M}$) is called a *cover* if the union of all the U_α for $\alpha \in \mathcal{M}$ is equal to S. From such a cover we form an abstract simplicial complex, called the *nerve* of the cover, by

$$\mathcal{C} = \left\{X \subset \mathcal{M} : \cap_{\alpha \in X} U_\alpha \neq \emptyset\right\}.$$

Thus $\{\alpha, \beta, \gamma\} \subset \mathcal{M}$ is in $\mathcal{C}$ precisely when $U_\alpha \cap U_\beta \cap U_\gamma$ is not empty. To see that $\mathcal{C}$ is an abstract simplicial complex we note that if $\{\alpha, \beta, \gamma\}$ is in $\mathcal{C}$ then we also must have $\{\alpha, \beta\}$ in $\mathcal{C}$ because if $U_\alpha \cap U_\beta \cap U_\gamma$ is not empty then also $U_\alpha \cap U_\beta$ is not empty.

In Fig. A1 we have a space covered by four subsets $\{U_\alpha, U_\beta, U_\gamma, U_\delta\}$ and the corresponding abstract simplicial complex is

$$\mathcal{C} = \left\{\{\alpha\}, \{\beta\}, \{\gamma\}, \{\delta\}, \{\alpha, \beta\}, \{\alpha, \gamma\}, \{\beta, \gamma\}, \{\alpha, \beta, \gamma\}, \{\gamma, \delta\}\right\}$$

Definition 6.
A map of abstract simplicial complexes $\Psi : (\mathcal{M}, \mathcal{C}) \to (\mathcal{M}', \mathcal{C}')$ is a function $\Psi : \mathcal{M} \to \mathcal{M}'$ so that on subsets if $X \in \mathcal{C}$ then $\Psi X \in \mathcal{C}'$.

For example we can take $\mathcal{M}' = \{\delta, \zeta\}$ and

$$\mathcal{C}' = \left\{\{\delta, \zeta\}, \{\delta\}, \{\zeta\}\right\}$$

and a simplicial map $\Psi : \mathcal{M} \to \mathcal{M}'$ could be given by $\Psi(\alpha) = \Psi(\beta) = \Psi(\gamma) = \zeta$ and $\Psi(\delta) = \delta$.

We can use maps of abstract simplicial complexes to implement hierarchies for information hiding or classification.

Definition 7.
A cover $\{W_k : k \in \mathcal{M}'\}$ of S is a *refinement* of the cover $\{U_\alpha : \alpha \in \mathcal{M}\}$ if there is a map $\Psi : \mathcal{M}' \to \mathcal{M}$ so that $W_k \subset U_{\Psi(k)}$. It then follows that Ψ is a map of abstract simplicial complexes from the nerve of the cover $\{W_k : k \in \mathcal{M}'\}$ to the nerve of $\{U_\alpha : \alpha \in \mathcal{M}\}$.

A.2. Realisation of abstract simplicial complexes in $\mathbb{R}^n$

The familiar xy plane for 2-dimensional geometry is called $\mathbb{R}^2$ as it uses two copies of the real numbers $\mathbb{R}$. Its elements are ordered pairs (x, y) for x and y real numbers. We have a basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$ and can write any point in the plane as $(x, y) = x\,e_1 + y\,e_2$. Similarly for 3-dimensional space $\mathbb{R}^3$ we have points (x, y, z), and if we use new basis elements $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$ we can write $(x, y, z) = x\,e_1 + y\,e_2 + z\,e_3$.

In (for example) $\mathbb{R}^3$ we have points which we call 0-simplices, e.g., e_1 and e_2. The 1-simplices are lines connecting the 0-simplices, e.g., $x\,e_1 + y\,e_2$ for real $x, y \geq 0$ with $x + y = 1$. The 2-simplices are triangles spanned by three vertices, e.g., $x\,e_1 + y\,e_2 + z\,e_3$ for real $x, y, z \geq 0$ with $x + y + z = 1$. We extend this to be 3-simplices being tetrahedra, etc. A 3-simplex is visualised in Fig. A1 where the vertices are labelled $\{\alpha, \beta, \gamma\}$.

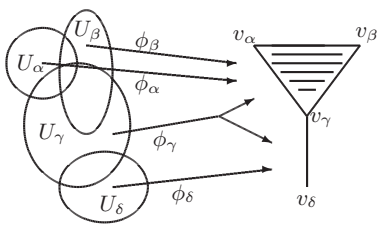

Figure A1. A simplicial complex and a partition of unity for a cover by four sets.

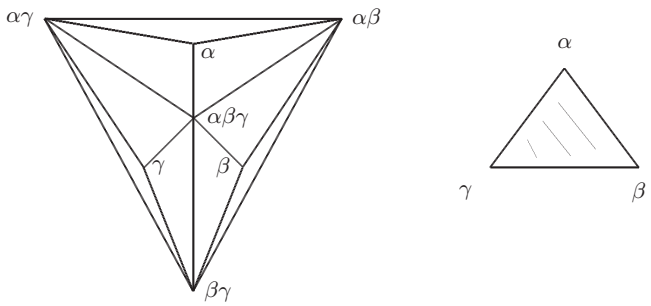

Figure A2. Comparing a single 2-simplex (right) and its graph (left).

An n-simplex will have *faces* which are simplices bounded by subsets of its vertices. Thus a 3-simplex will have one 3-face (itself), four 2-faces which are 2-simplices, six 1-faces which are 1-simplices and four 0-faces which are 0-simplices (vertices). In Fig. A1 the 2-simplex $\{\alpha, \beta, \gamma\}$ has a 1-face labelled by $\{\alpha, \gamma\}$ and a 0-face labelled by $\{\alpha\}$.

We can use this to define a higher dimensional analogue of a planar graph called a simplicial complex–a graph is an example of a simplicial complex which only contains 0-simplices and 1-simplices:

Definition 8.
A *simplicial complex* is a collection of simplices in some space so that the face of any simplex in the collection is also in the collection, and the intersection of any two simplices is a face of both of them.

Fig. A1 gives an example of a simplicial complex which is a union of a 2-simplex and a 1-simplex. These simplices intersect at the common 1-face e_γ.

There is a construction which will give a simplicial complex for every abstract simplicial complex in a functorial manner. In general, this construction uses very high dimensional spaces, which is usually not necessary in practice, but it simplifies the theory. Just as many (but not all) graphs can be drawn in 2-dimensional space we can often draw a simplicial complex in a dimension much smaller than that used in Proposition 1. The large space $\mathbb{R}^{\mathcal{M}}$ is a vector space with basis e_α for all $\alpha \in \mathcal{M}$.

Proposition 1.
To every abstract simplicial complex $(\mathcal{M}, \mathcal{C})$ (as in Definition 6) is associated its standard realisation $\Delta_{\mathcal{C}} \subset \mathbb{R}^{\mathcal{M}}$, as a simplicial complex. The simplex spanned by $X \in \mathcal{C}$ is

$$\Delta_X = \Big\{ \sum_{\alpha \in X} \lambda_\alpha \, e_\alpha : \lambda_\alpha \in [0,1], \ \sum_{\alpha \in X} \lambda_\alpha = 1 \Big\}.$$

Further, a map of abstract simplicial complexes $\Psi : (\mathcal{M}, \mathcal{C}) \to (\mathcal{M}', \mathcal{C}')$ can be extended to a map of their realisations as $\Delta_\Psi : \Delta_{\mathcal{C}} \to \Delta_{\mathcal{C}'}$ by defining

$$\Delta_\Psi \Big(\sum_{\alpha \in X} \lambda_\alpha \, e_\alpha \Big) = \sum_{\alpha \in X} \lambda_\alpha \, e_{\Psi(\alpha)}.$$

Proof: The simplex Δ_X is a $(|X| - 1)$-simplex where $|X|$ is the size of X, and if $Y \subset X$ then Δ_Y is a face of Δ_X. Then $\Delta_X \cap \Delta_Z = \Delta_{X \cap Z}$ and Definition 8 is seen to be satisfied. □

A.3. Covers and partitions of unity

Having created the geometric realisation of the simplex we are now able to use the categorisation of the data in the state space S according to a cover $\{U_\alpha : \alpha \in \mathcal{M}\}$ and its associated abstract simplicial complex $\mathcal{C}$, to create a geometric visualisation in $\Delta_{\mathcal{C}}$. To do this we need an appropriate map from S to $\mathcal{C}$ that contains the information $\phi_\alpha(s)$ which tells us how much we need to be concerned about α when in state $s \in S$ on a scale from 0 to 1.

Definition 9.
A *partition of unity* for the cover $\{U_\alpha \subset S \,|\, \alpha \in \mathcal{M}\}$ is a function $\phi_\alpha : S \to [0,1]$ for every $\alpha \in \mathcal{M}$ such that

(1) if $\phi_\alpha(s) \neq 0$ then $s \in U_\alpha$;
(2) $\sum_{\alpha \in \mathcal{M}} \phi_\alpha(s) = 1$ for all $s \in S$.

We then have a function $\phi : S \to \Delta_{\mathcal{C}}$ given by

$$\phi(s) = \sum_{\alpha \in \mathcal{M}} \phi_\alpha(s) \, e_\alpha.$$

Fig. A1 visualises a simplicial complex and partition of unity for a cover by four sets. Note that the triangle in Fig. A1 is shaded to form a 2-simplex precisely because $U_\alpha \cap U_\beta \cap U_\gamma$ is not empty. In specific circumstances we can impose extra conditions on ϕ, e.g., continuity or computability.

A.4. Belief

It is important to distinguish between belief in something and a probability that that thing occurs [26,27]. On being told by a completely reliable source that a person has a car which has a single colour, we could form two statements,

$B =$ 'the car is blue' and $NB =$'the car is not blue'.

The combination B or NB we would consider to have a belief of 1, but in the absence of any other information we would have no basis to assign a non-zero belief value to the separate statement B or to the statement NB. We could randomly assign belief values to each which added up to 1, but this would only undermine the idea that *belief ought be assigned according to evidence*. Sensibly our belief $\mathrm{Bel}(\{B, NB\})$ in (B or NB) is strictly greater than the sum of $\mathrm{Bel}(\{B\})$ and $\mathrm{Bel}(\{NB\})$. Such a conclusion means that we are not dealing with a probability distribution.

Definition 9.
We consider beliefs in a finite set X of statements. A *generalised belief function* on X is a function

$$\mathrm{Bel} : P(X) \to [0,1],$$

where $P(X)$ is the set of subsets of X. Furthermore, for the empty set $\mathrm{Bel}(\emptyset) = 0$ and the sets satisfy the 'super-additivity' property

$$\mathrm{Bel}(Y \cup Z) + \mathrm{Bel}(Y \cap Z) \geq \mathrm{Bel}(Y) + \mathrm{Bel}(Z) \quad \text{for all } Y, Z \subset X. \tag{1}$$

We denote by $\mathcal{B}(X)$ the set of belief functions on X.

We shall say that a belief function is *normalised* if $\mathrm{Bel}(X) = 1$. It is important to note that we do *not* impose this normalisation condition–hence our word *generalised* above. Thus, we reserve the right to believe that the set of presented alternatives X may be incomplete.

The 'super-additivity' property is simply justified in that, in addition to those people who believe in Y and those who believe in Z, there may be people who just believe that at least one is true.

A.5. Simplicial complexes and graphs

Graphs are a standard data structure in computer science. We claim that for certain purposes simplicial complexes are preferable. These purposes are related to the reasons why simplicial complexes were invented by topologists: In describing covers of spaces by subsets, these subsets can model multiple objectives or circumstances which can occur simultaneously. This intrinsically higher dimensional picture does not easily reduce to a graph. To see this, first consider this straightforward construction.

In transforming a simplicial complex to a graph,

(i) each mode/face f of the complex becomes a vertex v; and

(ii) each pair of nested mode/faces $f_1 \subset f_2$ of the complex becomes an edge $v_1 \to v_2$.

In summary:

Lemma 1.
An n-simplex contains $2^{n+1} - 1$ faces. To make a representation in a graph, the resulting graph would have $2^{n+1} - 1$ vertices.

In Fig. A2 we compare a simple 2-simplex $\alpha\beta\gamma$ to its graph, where we take the sub-simplices of $\alpha\beta\gamma$ and connect the intersections (= possible mode transitions) by a line in the graph. This shows the considerable increase in complexity on constructing the graph, even for one of the simplest simplicial complexes. The graphical representation of the simplicial complex in Fig. 3 would be much more complicated.

Not only is the graph more complicated, but it is much more difficult to interpret. A point on the 2-simplex (the filled in triangle) carries a large amount of information about the state of the system in how close to an edge or vertex it is. All points in the interior of the triangle correspond to the single vertex $\alpha\beta\gamma$ in the graph, so a position in a vertex of the graph loses this information. The discontinuous motion from vertex to vertex in the graph lacks any explainability or predictive value. This is in contrast to the continuous motion of a point around the 2-simplex, where at least a guess may be made about the likely future behaviour of the system.

References

1. Heyck H. *Age of system: understanding the development of modern social science*. Baltimore: Johns Hopkins University Press, 2015.
2. Nofre D. Content Is meaningless, and structure Is all-important': defining the nature of computer science in the age of high modernism, c.1950–c.1965. *IEEE Ann Hist Comput* 2023;**45**(2):29–42.
3. UK Government. *Fact Sheet 2: national security risk assessment*, 2022. assets.publishing.service.gov.uk/media/5a74ce6640f0b61df4778a5b/Factsheet2-National-Security-Risk-Assessment.pdf
4. Beggs EJ, Tucker JV. A model of systems with modes and mode transitions. *J Log Algebr Methods Prog* 2022;**127**:100774.
5. Yamin MM, Katt B, Gkioulos V. Cyber ranges and security testbeds: scenarios, functions, tools and architecture. *Comput Secur* 2020;**88**:101636. https://doi.org/10.1016/j.cose.2019.101636
6. Cabinet Office. *A strong Britain in an age of uncertainty: the national security strategy*. 2010. https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty
7. UK Home Office. *Critical incident management, Border force, immigration enforcement and UK visas and immigration*. Version 13.0, 2021.https://www.gov.uk/government/publications/powers-and-operational-procedure/critical-incident-management-accessible (25 July 2025, date last accessed).
8. BBC News. *Broadwater Farm riots: PC Keith Blakelock's 1985 murder recalled*. https://www.bbc.co.uk/news/uk-england-london-34433752 (25 July 2025, date last accessed).
9. Risk management. 2023. https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk (25 July 2025, date last accessed).
10. Rowe P, Damodaran S, Malinovsky P. A coordination model for attack graphs. MITRE, 2023. https://www.mitre.org/news-insights/publication/coordination-model-attack-graphs (25 August 2025, date last accessed).
11. Schneier B. Attack trees. *Dr. Dobb's J Software Tools* 1999;**24**(12):21–9. https://www.schneier.com/academic/archives/1999/12/attack_trees.html (25 August 2025, date last accessed).
12. National Institute of Standards and Technology. *Developing cyber resilient systems: a systems security engineering approach*. NIST SP 800D160. Washington, D.C.: U.S. Department of Commerce, 2021.
13. Perrett K, Wilson ID. A cyber resilience analysis case study of an industrial operational technology environment. *Environ Syst Decis* 2023;**43**:178–90. https://doi.org/10.1007/s10669-023-09895-1
14. Smith K, Wilson ID. Critical infrastructures: a comparison of definitions. *Int J Crit Infra* 2023;**19**(4):323–39.
15. National cyber security centre. https://www.ncsc.gov.uk/guidance/ceos-responding-cyber-incidents (25 August 2025, date last accessed).
16. Ozoran A, Cigdemoglu B, Ilgar CS. Economic, Socio-cultural and existential engagement strategies during COVID-19 Pandemic: a scenario-based experiment. *Int J Manag Stud* 2023;**30**(2):203–34. https://doi.org/10.32890/ijms2023.30.2.2
17. Sus M, Hadeed M. Theory-infused and policy-relevant: On the usefulness of scenario analysis for international relations. *Contemp Secur Policy* 2020;**41**(3):432–55.https://doi.org/10.1080/13523260.2020.1730055
18. Flynn M, Ford JD, Pearce T. *et al.* Participatory scenario planning and climate change impacts, adaptation and vulnerability research in the Arctic. *Environ Sci Pol* 2018;**79**:45–53. https://doi.org/10.1016/j.envsci.2017.10.012
19. Anderson GB, Barnes EA, Bell ML. *et al.* The future of climate epidemiology: Opportunities for advancing health research in the context of climate change. *Am J Epidemiol* 2019;**188**(5):866–72. https://doi.org/10.1093/aje/kwz034
20. Eilouti B. Scenario-based design: New applications in metamorphic architecture. *Front Archit Res* 2018;**7**(4):530–43. https://doi.org/10.1016/j.foar.2018.07.003
21. Bekkers R. Who gives what and when? A scenario study of intentions to give time and money. *Soc Sci Res* 2010;**39**(3):369–81. https://doi.org/10.1016/j.ssresearch.2009.08.008
22. Augier M, Dew N, Knudsen TN. Stieglitz. Organizational persistence in the use of war gaming and scenario planning. *Long Range Plann* 2018;**51**(4):511–25. https://doi.org/10.1016/j.lrp.2017.12.005
23. Carpenter SR, Pingali PL, Bennett EM. *et al. Ecosystems and human well-being: Scenarios*, Vol. **2**. Washington, DC: Island Press, 2005.
24. Diana F. *Our emerging future*. 2016. https://frankdiana.net/2016/04/21/our-emerging-future (25 August 2025, date last accessed).
25. Lee JM. *Manifolds and differential geometry*. Providence RI: Graduate Texts in Mathematics 107, A.M.S., 2009.
26. Shafer G. Perspectives on the theory and practice of belief functions. *Int J Approx Reas* 1990;**4**(5-6):323–62.https://doi.org/10.1016/0888-613X(90)90012-Q
27. Yager RR, Liu L. *Classic works of the Dempster-Shafer theory of belief functions*. Berlin-Heidelberg: Studies in Fuzziness and Soft Computing, Springer, 2008. https://doi.org/10.1007/978-3-540-44792-4