Cyber Resilience, Dependability and Security

Angela Mison[1], Gareth Davies[2] and Peter Eden[1]
[1]University of South Wales, Pontypridd, UK
[2]University of the West of England, Bristol, UK

angela.mison@southwales.ac.uk
Gareth13.Davies@uwe.ac.uk (corresponding author)
peter.eden@southwales.ac.uk

Abstract: There is a continuing skills shortage associated with digital security and DevSecOps (World Economic Forum, 2023), but this paper argues that is due to non-recognition that it is time for cyber security and/or digital security to be defined, and a further separation of specialisms in computing to be made apparent. This has become increasingly important when considering Artificial Intelligence. The problem is not new. This paper presents a refinement of the principles suggested by Milner (2007) of using a model to describe behaviour and organise software, grappling with seemingly intractable and complex problems which cross boundaries between different systems: engineering, technological, social, economic, legal, and political, each with a distinct perspective and goal. It emphasises Hoare's (1996) assertion that system failures are largely due to failed analysis impacting development of resilient systems. It argues that there are dichotomies between resilience – a system security/safety perspective, dependability – a user/consumer perspective, and security – a technology perspective. Many proposed systems to date have conflated these perspectives in the secure by design paradigm which requires a depth of knowledge and expertise. Unicorns are rare. This paper suggests how to overcome the skills shortage utilising the skill sets that are available in a manner that maximises the contribution to digital security. Recognising that not everyone and everything needs to communicate with the world reduces complexity and can increase trust. Concentration on the operational purpose of a system, resulting in an Operational Design Domain (ODD) reduces complexity further. Additional reduction in complexity is achieved by placing resilience in an engineering and programming development context, grounded in acceptable behaviours, while accepting dependability as a user expectation of system behaviour, and cyber security as a separate specialism addressing access to systems and infrastructure. Much of this paper is a reversion to defensive programming through the ODD. There is a need for any solution to the skills shortage be scalable and economic, and this paper suggests how that can be achieved using existing skill sets targeted at their specialisms.

Keywords: Cyber security, Resilience, Dependability, Digital forensics

1. Introduction

There is a myriad of definitions of cyber security, itself, part of the problem. The top Google search engine returns for a definition of cybersecurity demonstrates the subtle differences in emphasis and understanding of the term.

From the NCSC's (2023) reduction of risk, itgovernance.co.uk's (2023) the application of technologies, processes and controls, CISA's (2023) 'protection of networks devices and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity and availability of information', to Kaspersky's (2023) 'cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks', the definitions highlight the priority of the technology element of organisations concerned and/or their starting point.

The paradigm of security by design (His Majesty's Government, 2023) is an attempt to solve the cyber security issues no matter the priority or starting point indicated above. The Cybersecurity and Infrastructure Security Agency (CISA) is making a series of recommendations, attempting to transfer the majority of the responsibility for software from the end user to the provider (Riotta, 2023). The issues are complicated by the ubiquitous nature of systems, the promotion of hyperconnectivity as a business benefit and the use of Agile technologies to maximise those hypothesised benefits (McKinsey, 2022).

Something very few wish to address is the building of new systems which interact with or depend on legacy systems, where the knowledge and expertise for those systems has long since departed and the documentation may be inadequate. Legacy systems are likely to perform a fundamental function within an organisation, which is both an advantage and disadvantage . The fact that they continue to function can leads to lack of investment until circumstances combine to produce a catastrophic meltdown (Charette, 2014). The identified benefit of retaining legacy systems can be that their very historical nature can renders them arcane and in some cases, unknown to even insiders, through contemporary unfamiliarity with the logic, languages and technologies supporting those legacy systems (King, 2022). Hitherto, malefactors seem to have ignored critical infrastructure legacy systems, looking for easy pickings and higher returns, but now, they are viewed as a less secure and a simpler way to gain access to more secure systems with returns due to ransomware (Raywood, 2023).

To place any system in its operational context, the term digital security is equally relevant and reflects the impact of systems, their use on a daily basis, and the dependence of society on their availability and integrity, either directly or indirectly. Perhaps, having the broadest perspective, the Organisation for Economic Cooperation and Development (OECD) (2023) has an apt definition of digital security and takes an economic and societal interpretation, that extends cyber security to consider impact. The OECD definition includes "the economic and social aspects of cybersecurity, as opposed to purely technical aspects, … 'digital' is consistent with expressions such as digital economy, digital transformation, and digital technologies. It forms a basis for constructive international dialogue between stakeholders seeking to foster trust." This definition is the basis of creating the ODD and its operational boundaries. The ODD is derived from the fundamental understanding of the purpose and expected behaviour of a system.

There are other broader perspectives of cyber security, and this includes those who control budgets and those concerned with the societal impacts attributable to failures of traditional cyber security. As an example, having the ears of Boards and Executives, cyber security can be seen as "not just about managing risk, it's also a strategic issue that shapes product capability, organizational effectiveness, and customer relationships, … identifying where the business creates value and analysing threats, … [working] to de-risk enterprise platforms, extract value from existing investments, secure value chains, and embed 'security by design' into new products and businesses" (Mckinsey.com, 2023). From the McKinsey statement it can be seen that consequences of a successful cyber attack may represent existential risks to organisations .

Further difficulties are caused by the lack of understanding and distinguishing between the ill-defined concepts of information warfare and cyber warfare. The two combine in digital warfare, whether the protagonists are nation states, organised crime groups, guerilla crime groups using Crime as a Service, or individuals demonstrating their capability. Everything in cyberspace is fair game. Access is the objective. What comes after that is opportunistic.

2. An Alternative Approach to Addressing the Skills Shortage

It may seem strange to suggest that the solution to the skills shortage in cyber security could be addressed by revisiting exactly how systems are developed, maintained, and updated. Taking advantage of the existing skills and strengths of the existing personnel, can result in the matching of those skills and strengths appropriate to the lifecycle phase (Paulsen & Byers, 2019). A common vocabulary for qualities of systems is needed (US Food and Drug Administration, 2023). The establishment of common vocabulary lends itself to the matching of which skill sets are required, where and when. Doing this, ensuring common understanding, enables the complex task of achieving maximum cyber security to be achieved, particularly when discussions cross skills boundaries

Part of the problems associated with the skills shortage is the overwhelming nature of imposing 'cyber security' over an organisation and its systems, and the experience and knowledge of detail required by those responsible for their defence.

Simplifying the problems, analysis, to just resilience and security results in the realisation that there are organisational operational / functional applications, based on the purpose of the organisation, and the infrastructure, which becomes the responsibility of cyber security and includes operating systems, standard applications eg word processing, spreadsheets, etc, networks and devices. They can be identified through recognising what system or application is organisation specific and requires knowledge of that data that is moving through the system, the underlying processes, and to whom the data should be communicated. This process definition assists in the establishment of virtual networks and identification of endpoints which become the responsibility of cyber security.

Secure by design (His Majesty's Government, 2023) remains aspirational. It requires everyone involved from the Board to the end user to be able to understand an ill-defined, nebulous, and multiway interpretable security when they are doing whatever task is allocated. This implies a knowledge of both the system and cybersecurity requirements that they may not have. Even more telling, is the impossibility of ensuring they are all aware of the requirements of digital security.

More applications are being developed that contain an element of intelligence. In advance of mass applications being developed, the mantra of 'Responsible AI by design' paradigm (Lu et al., 2023), demonstrates the future difficulties for cybersecurity and digital security as ever more complicated and complex than current circumstances due to machine learning, evolution and the requirement for both audit and transparency of algorithms. This is not only for the organisation but extends to the requirement for forensic explainability should a system ever be associated with an adverse event or decision.

While this paper suggests a possible approach to addressing the skills shortage, at this point, it is worth introducing the caveat in regard to AI. If the AI system is to evolve while in operation, it is not necessary to gain access to the internals of the system to corrupt it, merely to influence its learning. At this time, no solution is completely foolproof in protecting against adversarial machine learning. In the same way that misinformation and disinformation can affect human thinking and learning, the same is true for AI. That systems are open to system on system psy ops is the province of the military industrial complex.

However bad the skills shortage is now, it is likely to get worse. How much more knowledge is expected of these omniscient unicorns? Current practice is linked with extending their expertise rather than on concentrating on what is within their skill set and, for a change, enabling them to contribute to the delivery of a system that works and meets its objectives in a way that is judged as successful. According to Gartner (Panetta, 2021), "48% of CIOs and technology executives having deployed or planning to deploy [AI] technologies in the next 12 months."

Figure 1 suggests the skills split between business functions, systems development, and cyber security. It should be noted that the behaviour required to achieve business objectives is defined through process definition, leaving the developer to exercise the skills of coding the process to achieve the required behaviour. Securing the Application Program Interface (API) of organisation specific systems also occurs within development as the parameter sets within the ODD become known.

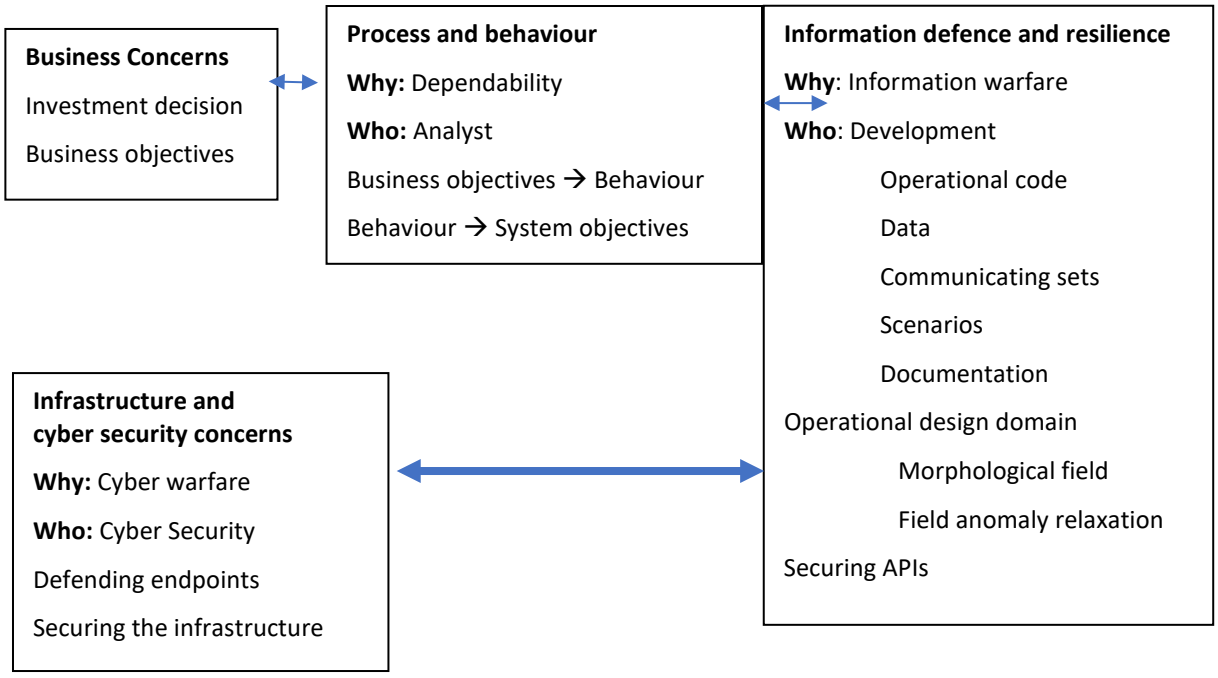

Figure 1: The who, what and why of digital defence, distinguishing necessary skill sets

3. Dependability, Analysis, and the Expected Behaviour of a System

Dependability is defined as "the quality of being able to be trusted and being very likely to do what people expect" (Cambridge English Corpus, 2023). This relates to the behaviour of a system.

Reduction of complexity argues that dependability is an end-user perspective which should be covered through analysis. Satisfaction of this results in a system that works according to everyone's or everything's expectation. Even if incorrect parameters or timings for execution are presented to the system under consideration, the system should continue to behave, in an expected manner. It may do so in a reduced capacity and/or capability, or degrade gracefully but will, otherwise, behave in an expected manner or advise the end-user of an error to avoid resistentialism (Deutscher, 1956).

It is unlikely that many considered the consequences of the UK's National Air Traffic Services (NATS) reaction to an inconsistency and safety concern to be acceptable behaviour. The cause was a single aircraft's flight details which caused the NATS system to shut down and move to a backup system which could remain operational for four hours. NATS quickly realised that it would take longer than the time available and transitioned to manual

input of flight plans. While there is sympathy for NATS being subject to Finagles Law of Dynamic Negatives (techopedia, 2021) on a peak travelling day of the year, there must be approval of their safety considerations. No one wants a midair collision. The repercussions in the broader context were financially staggering and took a minimum of three days to resolve due to positioning and capacity issues (Hand, 2023). To demonstrate where safety is an ostensible imperative, but where limitation of scenario development was even more catastrophic, a Cruise autonomous vehicle operating in San Francisco was involved in a collision with a pedestrian. The process defined that the vehicle should move to the side of the road to prevent a build up of traffic. Sensible, but the unfortunate pedestrian was lying, undetected, under the vehicle (Brodkin, 2023) which was not subject to manual intervention.

Analysis has a dual aspect, defining system objectives and defining behaviour contributing to the achievement of those objectives. The objectives are set by the organisation, whether it is increasing functionality or maximising the benefits of surveillance capitalism. The question for the analyst is not 'What is the system going to do?', but 'Why has the organisation committed to this investment and what does it expect to achieve?'. For an end-user, the behaviour of the system, linked to process definition, as in 'Who has to do what?' will either achieve or contribute to the objectives defined through the behaviour of the end-user, independent of this being a human or sub-system, in response to system demands. Dependability can be seen as predictability for the end-user in completing any system-based task. Where the end-user is a sub-system, the expected inputs and outputs should be defined in that outputs contribute or act as inputs to the next step and should be dependable in their own right.

The analysis is where systems often fail. As identified by Hoare (1996), "Programs have now got very large and very critical ... There have been many problems and failures, but these have nearly always been attributable to inadequate analysis of requirements or inadequate management control." Too often analysts are faced with a situation in which protagonists define a 'normal or standard operation' for a process, but then tack on the phrase, 'but, sometimes….'. The 'sometimes' are, in reality, extensions to the base case and more properly the subject of scenario definition and development as they impact the operational design domain (ODD), a "set of operating conditions under which a given … system … or feature thereof is specifically designed to function" (ISO/TC 204 Intelligent Transport Systems, 2022). It should be recognised that any system development has its origins in an objective whether it is to make the system more secure or efficient, or to enable evolution or expansion of it, or an organisation, some way. This makes it an organisational project which contributes to the objectives of the organisation. That project requires iterative analysis in which the sponsors of the project need to be committed and have their time allocated to the project.

4. Resilience, Safety, and System Development

Resilience is defined as "the quality of being able to return quickly to a previous good condition after problems" (Cambridge English Corpus, 2023). Resilience is covered in development in collaboration with analysts in respect of behaviours resulting from specific scenarios outside the core ODD as defined by the initial analysis.

The initial analysis defines the system in its optimum working state - a standard process with no variation and everything working as defined. The element of failure of analysis arises here, in the variation of system operation to accommodate scenarios which, deriving from field anomaly relaxation, due to lack of iterative analysis input. Habitually there is a single analysis, and a contributing lack of commitment from commissioning entities.

When presented with an incomplete first pass analysis, developers may make logical decisions based on insufficient input which may contribute to the failure of the system when deployed. However intuitive and logical a decision may appear to a developer, in any deployed system, it may be completely counterintuitive to the ultimate end-user or even, the organisation, thereby marring its dependability through resultant unexpected behaviour. Murphy's Law (2012) applies. Further analysis and commitment from the commissioning entity may be necessary during the definition of scenarios which in effect relate to the development of contours within the ODD from mild variation to incipient failure.

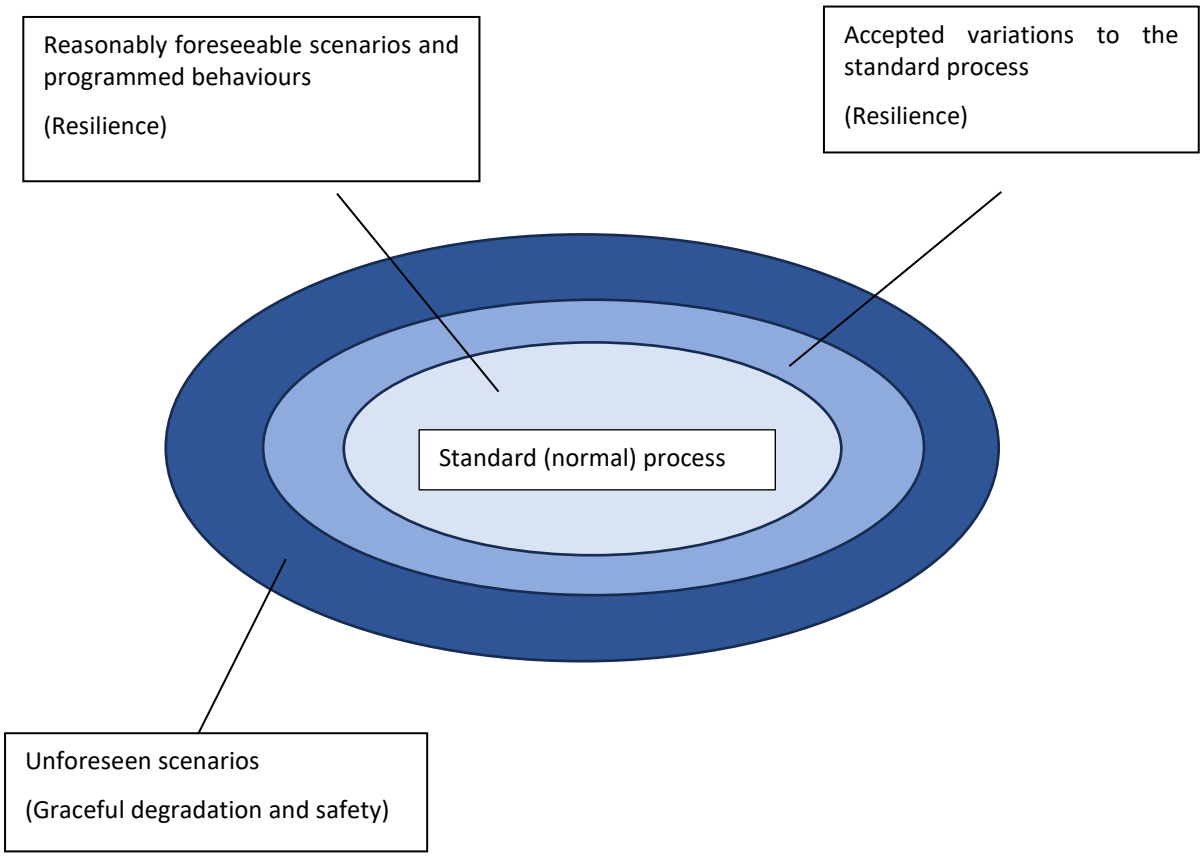

Figure 2: Example of operational design domain contours

Referring to the NATS failure, it is disconcerting to be in a chaotic situation, as has happened historically in some airspaces, where pilots continually need to broadcast their positions in an effort to avoid mid-air collisions and provide the air traffic information to others in the air. The solution to the NATS failure is simple in retrospect. It involves a pre-screening of flight data and the rejection of those not in compliance with expectations of the ODD, either acceptable parameters, or failure due to other errors. They are not presented to the system proper. Rather than the entire system transitioning to manual operation, it is the rejected flight data that is dealt with manually while all other flights continue to be processed automatically. This type of event or scenario has been stated, by NATS, as having an extremely low probability which would place it in the outermost reaches of the ODD contours unless pre-screened. The logic of determining behaviours attributable to the ODD Contours is limited by the developers' and analysts' imaginations of the 'What if …' situations, as demonstrated by the Cruise autonomous vehicle.

In terms of scenario definition, this is to put the system into the real world where acceptable, random and unpredictable acts happen. It also entails using the imaginative and creative powers of future gazing by developers and analysts. It is useful to consider scenarios and decision making as based on game theory and statistics, which have sound mathematical foundations although it should be recognised that use of Bayesian statistics may result in inconsistencies and non-determinism as probabilities are calculated to include historical choices. The end result is a lot of defensive programming which, with luck, will be used rarely.

In terms of defining operational design contours, these are dependent on scenarios relevant to the system under consideration, their probability of occurrence, and priority. There can be as many as necessary, and each contour can be subject to testing, or used to define the test suite, thereby ensuring that at each level the system works behaviourally as defined in the analysis. Defining test suites in line with operational design contours enables the test team to simplify the view of the system and ensure that a complete testing of the system is carried out.

As an example, a new user, despite any training, may attempt to input incorrect data. The engineering practices of Field Anomaly Relaxation (Nazmiye, et al., 2020) to determine scenarios, and/or creating a Morphological

Field, a component of general Morphological Analysis (Ritchey, 2022), can form the basis of judgement and audit as to resultant behaviour, and risk minimisation, lending itself to the future requirement of explainability of the system and its behaviour, in forensic circumstances. This becomes even more relevant and important when AI is added to the mix.

5. Information Defence, Data Flows and Intra-System Communication

The climate of information warfare exists and although the concepts are well understood, through laissez faire or lack of capability, organisations and systems continue to be subject to exploitation of vulnerabilities (Stupples, 2015). Whether it is organised by nation states, organised criminal groups, unethical competitors, or as guerilla tactics, it is for developers to implement API security to combat information warfare and for cyber security to implement defence mechanisms against cyber warfare for the infrastructure.

In addition to the elements of defining the ODD and its contours, information defence becomes part of business continuity. Developers are aware of who should be communicating with whom through the formation of virtual networks from their associated communicating sets. The ODD provides the list of acceptable operational parameters, or parameters for which there is a programmed resolution and behaviour.

Under these conditions, it becomes possible for developers to consider the failure of cyber defence in which a malefactor has gained access to the organisation's operational systems. The developers can include algorithms at the API, which identify rogue parameters putting the systems under threat. These rogue parameters may include source, destination, timing, or input or output parameters outside those within the ODD contours. These algorithms can initiate isolation of source and automatically advise cyber security of a potential breach and discovery location – removal of the domino in the race which halts a race in its tracks. It should be noted that the term 'isolation' is used, in this paper, to refer to a system or component part of a system rendering it unable to communicate or interact with other parts of the system.

Information security is built around the priorities determined by the organisation, addressing issues proactively rather than reactively as currently occurs. This can be done only in the knowledge of the system, its objectives, and its context of operation. It derives from the concept of 'defending' cyber assets (Aguiar, 2023), (NIST Computer Security Resource Center, 2023), as opposed to cyber infrastructure.

6. Cyber Defence, Endpoint Security and Segmentation

Future attacks and attackers cannot be known. A system must be defended continuously, against all malefactors and errors, and notify its defenders of the system location when it has been breached or subject to an attempted breach. For this reason, the collaboration between the developers who have documented the data flows and necessary communicating parties in any process provides the knowledge of the system, its priorities and weak points to those responsible for the overall defence of the organisation's digital assets. Depending on the level of security required, data flows, the responsibility of developers, can be validated at the API through resilience initiatives and use of isolation, while access to the network can be controlled by cyber security.

Where there is a need for universal access, as in random customer access to a retail website, reference can be made to the behavioural characteristics expected of the end-user, the customer. Where this deviates from the prescribed behaviour, as happens in many fintech applications, a limited number of attempts can be acceptable, or the end user can be locked out and a procedure usually requiring human customer/customer service interaction/intervention, must be completed before the lock is removed.

It can be seen from the foregoing, that digital access can be treated in much the same way as resilience through the definition of scenarios and access contours. The worst case scenario being segmentation of the external network through exclusion of all communications both to and from an offending party. Here, the slight repurposing of a Morphological Field would indicate the addresses and functions affected, which in turn relates to the potential isolation of a component of a system as it becomes non-functioning in the absence of available data.

In cases where on-going communication between parties is essential, back up lines of communication, person-to-person, can be triggered. Such communication, if technology based would require an alternative mechanism for communication, such as a land line, or satellite phone. The matching of the cyber defence contours together with the information defence contours defines, completely, the requirement and priority for the initialisation of business continuity procedures.

These arrangements are fully within the expertise of cyber defence, and do not require detailed knowledge of organisation specific systems beyond that. It demonstrates the importance of interactions with other areas of expertise and knowledge, but these interactions are between similarly educated and linguistically inclined personnel, although emerging from their education into different spheres.

7. Conclusion

There is increasing dependence on ubiquity and availability of systems, from society as a whole, down to individual organisation. Oftentimes, the concept of system unavailability seems completely alien and beyond comprehension. Historically, systems development and budgets have been pared to the bone. Simply put and referring back to Hoare (1996), secure systems cost more in the initial stages, which can be protracted.

A major contributing factor to losing track of systems and increasing organisational vulnerability, both in terms of interconnection and infrastructure, is the time lag relating to documentation resulting from the Agile, digital transformation push promoted by reputable management consultancies. Boards believe that Agile development is both cheap and quick, an essential component to the much promoted monetisation and efficiencies available from digital transformation and hyperconnectivity. Someone in IT and cyber security needs to convey to the Board that systems will cost more, in sheer documentation terms, if they are to be as secure as possible.

As a caveat, there is an expectation of the continuous availability of cyber defence staff and incident response teams. Reality can intervene. The current political situation in the United States of America may well provide an opportunity for its traditional and non-traditional enemies to launch cyber attacks while politicians argue over budgets and there is a potential for government shutdown. The implications of a shutdown, for any military in action, are more than significant, and potentially disastrous. This is a policy issue outside the control of any cyber defence unit. For national security, it is elements such as this that define the operational context and provide asymmetric advantage to adversaries.

References

Aguiar, A., 2023. *Defining Assets in Cybersecurity Asset Management.* [Online] Available at: https://noeticcyber.com/defining-cyber-asset-management/[Accessed 8 December 2923].

Brodkin, J., 2023. *After robotaxi dragged pedestrian 20 feet, Cruise founder and CEO resigns.* [Online] Available at: https://arstechnica.com/tech-policy/2023/11/after-robotaxi-dragged-pedestrian-20-feet-cruise-founder-and-ceo-resigns/[Accessed 8 December 2023].

Cambridge English Corpus, 2023. *Cambridge Dictionary.* [Online] Available at: https://dictionary.cambridge.org/dictionary/english/dependability[Accessed 25 September 2023].

Charette, R., 2014. *RBS Group Facing Huge Fine over Massive 2012 IT System Meltdown . Bank still fixing decades-long neglect if IT system infrastructure.* [Online] Available at: https://spectrum.ieee.org/royal-bank-of-scotland-group-facing-huge-fine-over-2012-massive-it-system-meltdown[Accessed 6 December 2023].

Cybersecurity & Infrastructure Security Agency (CISA), 2023. *What is cybersecurity.* [Online] Available at: https://www.cisa.gov/news-events/news/what-cybersecurity

Deutscher, I., 1956. Physicians' Reactions to a Mailed Questionnaire: A Study in 'Resistentialism.. *The Public Opinion Quarterly,* 20(3), pp. 599-604.

Hand, J., 2023. *Nats air traffic control: Experts reflect on three days of chaos.* [Online] Available at: https://www.bbc.co.uk/news/uk-66685349[Accessed 25 September 2023].

His Majesty's Government, 2023. *Secure by design.* [Online] Available at: https://www.gov.uk/government/collections/secure-by-design[Accessed 25 September 2023].

Hoare, C., 1996. *Unification of Theories: A challenge for Computing Science.* s.l., Springer Verlag, pp. 49-57.

itgovernance, 2023. *What is Cyber Security? Definition and Best Practices.* [Online] Available at: https://www.itgovernance.co.uk/what-is-cybersecurity

Kaspersky, 2023. *What is cyber security?.* [Online] Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security[Accessed 25 September 2023].

King, A., 2022. *https://www.securityindustry.org/2022/10/14/legacy-systems-rip-and-replace-or-keep-them-going/.* [Online] Available at: https://www.securityindustry.org/2022/10/14/legacy-systems-rip-and-replace-or-keep-them-going/[Accessed 8 December 2023].

Lu, Q., Zhu, L., Xu, X. & Whittle, J., 2023. Responsible-AI-by-Design: A Pattern collection for designing responsible artificial intelligence systems. *IEEE Software,* 40(3), pp. 63-71.

Mckinsey.com, 2023. *Cybersecurity.* [Online] Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/mckinsey-technology/overview/cybersecurity [Accessed 25 September 2023].

McKinsey, 2022. *The data-driven enterprise of 2025.* [Online] Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025 [Accessed 15 March 2022].

Milner, R., 2011. *Transcription of the Presentation Is Informatics a Science.* [Online] Available at: https://markstaples.com/files/Is%20Informatics%20a%20Science%20-%20v1.0.pdf[Accessed 27 April 2023].

Murphy, C. E., 2012. *Murphy's Laws Origin.* [Online] Available at: https://militaryhumor.net/murphys-laws-origin/[Accessed 9 September 2021].

National Cyber Security Centre (NCSC), 2023. *What is cyber security.* [Online] Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

National Cyber Security Centre, 2019. *Secure design principles.* [Online] Available at: https://www.ncsc.gov.uk/collection/cyber-security-design-principles[Accessed 24 October 2022].

NIST Computer Security Resource Center, 2023. *asset definitions.* [Online] Available at: https://csrc.nist.gov/glossary/term/asset[Accessed 8 December 2023].

OECD, 2022. *Digital Security.* [Online] Available at: https://www.oecd.org/digital/digital-security/[Accessed 8 December 2023].

Organisation for Economic Cooperation and Development (OECD), 2023. *Digital Security.* [Online] Available at: https://www.oecd.org/digital/digital-security/[Accessed 25 September 2023].

Panetta, K., 2021. *IT Budgets are Growing. Here's Where the Money's Going.* [Online] Available at: https://www.gartner.com/en/articles/it-budgets-are-growing-here-s-where-the-money-s-going[Accessed 25 September 2023].

Paulsen, C. & Byers, R., 2019. *NIST IR 7298 Rev. 3 Glossary of Key Information Security Terms.* [Online] Available at: https://doi.org/10.6028/NIST.IR.7298r3 [Accessed 8 December 2023].

Raywood, D., 2023. *What are the biggest threats to OT?.* [Online] Available at: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/operational-technologies-biggest-threats.html[Accessed 8 December 2023].

Riotta, C., 2023. *The nation's cyber defense agency is continuing to drive a major effort to shift security responsibilities from users to software providers.* [Online] Available at: https://www.nextgov.com/cybersecurity/2023/09/cisa-plans-new-secure-design-guidance/390019/[Accessed 25 September 2023].

Ritchey, T., 2022. General Morphological Analysis: An overview. *Academia Letters*, January, p. Article Number 4620.

Stupples, D., 2015. *What is information warfare?.* [Online] Available at: https://www.weforum.org/agenda/2015/12/what-is-information-warfare[Accessed 25 September 2023].

techopedia, 2021. *Finagle's Law.* [Online] Available at: https://images.techopedia.com/definition/19342/finagles-law[Accessed 9 September 2021].

US Food and Drug Administration, 2023. *Glossary of Computer System Software Development Terminology (8/95).* [Online] Available at: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-guides/glossary-computer-system-software-development-terminology-895[Accessed 8 December 2023].

World Economic Forum, 2023. *The Future of Jobs 2023,* Geneva: World Economic Forum.