



Physical Critical Infrastructure Protection - Security by Obscurity is No Defence for Western Survivability

Authors

Ian Saunders

Director Defence Systems, Soteria Shielding Ltd. and Visiting Fellow, Cranfield University.

Soteria Shielding Systems Ltd., 1 Canada Square, Canary Wharf, London, E14 5AB

is@soteriashielding.com

Prof. Gareth Appleby-Thomas

Professor of High Strain-Rate Material Responses for Defence Applications.

Defence Academy of the United Kingdom, Cranfield University, Shrivenham, Swindon, SN6 8LA, UK.

g.thomas@cranfield.ac.uk

Our Critical Infrastructure enables us to not only live and prosper but also defend the complex societies that we have created.

1. Abstract

Critical Infrastructure - the systems, facilities and assets that are vital for the functioning and protection of society and the economy.

The aim of this white paper is to undertake a broad analysis of the threats to Critical Infrastructure and how western democracies address them, alongside highlighting the enormity and the complexity of the issue, hopefully prompting new dialogue and, more importantly, action.

For the purpose of this paper, the authors have identified four vectors that define the threats relevant to critical infrastructure (Fig. 1).

Fig. 1: Four vectors defining threats to critical infrastructure

Physical Attack Vector	Threats of an aggressive nature targeting the physical properties, operability and capabilities of critical infrastructure.
Cyber Attack Vector	Threats of an aggressive nature targeting the online programs, protocols and technological capabilities of critical infrastructure.
Adverse Weather Vector	Threats of a non-confrontational, destructive nature inflicted by adverse weather on the operability and capabilities of critical infrastructure.
Structural Decay Vector	Threats of a non-confrontational, destructive nature caused by the decay and erosion of the physical properties of critical infrastructure.

The increasing volume of academic research into the critical infrastructure ecosystem, as referred to later in this paper (Fig 10.) is a tangible indicator of its importance, particularly the patterns emerging from Chinese institutions. The question of whether this evolving research is from a futureproofing/defence perspective or to greater understand the weakness of other nations is beyond the scope of this paper; it does however demonstrate a desire for increased knowledge and therefore capability.

As a current example, the targeting of Ukrainian critical infrastructure by Russian forces demonstrates the importance of this arena, with such infrastructure now clearly

identified as battlefield assets with game-changing strategic and psychological potential worthy of high levels of defence and a 'building back better' mindset.

Drilling down into the threats affecting the critical infrastructure ecosystem, we observe that the challenges facing the two attack vectors are neither exclusively civil nor exclusively military but both, in the context of what has been termed 'total war'.

Indirectly, the same could be said of the two non-confrontational vectors.

In the current geo-political climate, we are once again at a point where we must protect civilian assets from potential overt military, terrorist and covert aggression; our enemies are both seen and unseen. Due to the complex nature of the threats against critical infrastructure, the non-confrontational vectors, arguably both man-made and natural, require an almost identical style of response to those of the physical attack vector – namely enhanced physical resilience.

Enhanced physical resilience is a passive form of defence and comes in the form of greater protection. As an example of the inherent importance of this approach, it is applicable even to elements of the seemingly less tangible 'cyber' domain. While the cyber-attack vector is proactively defending against attacks online and supported by a combination of public/private sector investment, tech development and constant deployment, the hardware, power and communications aspects of the cyber threat are at constant risk and require effective physical protection against converging threats.

The authors have developed the Critical Infrastructure Threat Prism to highlight the protective synergy across the western powers at the strategic and operational levels. Only in the cyber-attack vector, however, is there any collective Critical 5 tactical level guidance or action in the form of the recent recommendation to include 12 essential security elements into all official and corporate Operational Technology (OT) procurement, as a minimum cyber security requirement.

The Critical 5 nations have made no mitigation recommendations for the physical attack vector in relation to minimum physical resilience guidelines for critical infrastructure, nor the non-confrontational threat vectors relating to adverse weather and structural decay. This oversight could dramatically affect the defence capabilities of both the Five Eyes Alliance and NATO as well as the domestic operability of member states' - built infrastructure, critical or otherwise.

The basic three-phase analysis of each critical infrastructure vector in this paper has also highlighted similar patterns of underreach in relation to the proactive hardening of physical critical infrastructure as a passive defence against attack and wider protection against adverse weather and structural decay.

Contents

1.	Abstract	2
	Fig. 1: Four vectors defining threats to critical infrastructure	2
2.	Introduction.....	5
3.	Defending Democracy.....	6
4.	Critical Infrastructure Definition and Deployment.....	6
5.	A Sovereign Perspective and Critical 5.....	7
	5a. The United Kingdom:	7
	5b. The United States:	9
	Fig. 2: The 16 US Critical Infrastructure sectors and the Sector Risk Management Agencies (SRMA) which are responsible for their coordination, management and reporting to the national Cyber Security Infrastructure Security Agency (CISA).....	10
6.	Critical Infrastructure Threat Response - Analysis.....	11
	Fig. 3: Critical Infrastructure Protection - Direction of Travel	12
7.	Identified Threat Vectors	12
	7a. The Critical Infrastructure Threat Prism (CITP)	13
	Fig. 4: Critical Infrastructure Threat Prisms	14
	7b. The Cyber Attack Vector.....	15
	7c. The Physical Attack Vector	17
	Fig. 5: The nominal physical (velocity) threat regimes against critical infrastructure.	18
8.	Critical Infrastructure Interdependence (CII) and Threat Realization	20
	Fig. 6: Illustration of the interdependency between Critical Infrastructure assets.....	21
9.	Owning and Influencing the Defence Space	21
10.	Non-Confrontational Threats – Adverse weather and structural decay	23
	Fig. 7: Cascading effects of localised failure.	24
11.	Threat Convergence	25
	Fig. 8: Critical Infrastructure relationships within a Cyber-Physical System (CPS).	29
	Fig. 9: CISA “Framework for Aligning Security Functions” (2021).	30
12.	Critical Infrastructure Reliance, Destruction and Defence – A Subject of Rapidly Emerging Interest.....	28
	Fig. 10: Trends in publication of peer-reviewed academic papers post-2000 focused on ‘Critical Infrastructure’	29
	Fig. 11: Funding body data for articles explored in Fig. 10.	30
13.	Summary.....	30

2. Introduction

Throughout human history we have developed the tools, industry and technology to support our constantly increasing demands, demands that today may arguably exceed our needs/ability to properly sustain them, but which have been responsible for our evolution as the world's dominant species. Such advancements, however, have not only become an integral part of our ultra-connected lives but essential to our stability and ultimate survival.

Communication, health, energy, water and defence are just a few of the sectors identified as paramount to both our day-to-day existence and our long-term evolution. Increasingly, nations are defining the infrastructure assets that facilitate these sectors as critical under national legislation and in doing so have realised that many are exposed to a range of threats, from violent attack and structural erosion to extreme weather conditions. It has become an undeniable fact that, unlike some of our enemies, western democracies can no longer live without the technology and systems that now manage our daily lives. They have become critical to our survivability; they ensure our family, society and sovereign stability and their evolution has protected us since the days of the industrial revolution.

Our nation's dependence on the built infrastructure and technology facilitating these critical requirements is now paramount. However, they are not only our greatest assets but also our "Achilles heel" - our "weakest link". We can no longer live, govern and function without the critical infrastructure which we continue to develop, but do not continue to protect.

Since the early 2000s (and particularly post-2014, corresponding to the Russian invasion/occupation of Crimea) there has been an increasing amount of detailed academic research and much debate on the identification, acceptance and creation of policy on Critical Infrastructure protection/defence. The cyber ecosystem has, quite rightly, received a lot of attention due to a constant stream of attacks ranging from lone-wolf hackers to aggressive state interference. In comparison very little attention has been given to the threats that physical Critical Infrastructure now faces across our ultra-connected cultures and societies.

This oversight must be corrected if we are to avoid the dire consequences of cascading infrastructure failure resulting in widespread disruption to our civilian and military landscapes and threatening our ultimate survivability. Physical Critical Infrastructure Protection is now one of the seminal and under-resourced security issues of our day,

essential to address if we want to deny our enemies high impact soft targets and protect our societies against increasingly violent and adverse weather. The consequences of not protecting our built critical infrastructure can range from shifts in the geopolitical order to large scale humanitarian suffering, social instability, economic shutdown, and the breakdown of law and order. **Physical critical infrastructure protection is the protection of our entire way of life.**

3. Defending Democracy

Conflict is changing rapidly, once again bringing battlefield-level threats to the towns and cities of Europe. The large-scale use of unmanned aerial vehicles (attack drones), the enhanced capabilities of previous low-tech munitions in the form of glide bombs and the deniable targeting by aggressive states of vital undersea assets are all designed to weaken critical infrastructure, sovereign defences, and the human will to win.

As stated in the abstract of this document, critical infrastructure is the platform through which we are able to defend our societies and cultures: from the facilitation of defence policy to the asset development and manufacturing of the defence industrial base, from the recruitment, training, and accommodation of personnel, to the defence bases and establishments where the operability of defence hardware is maintained at readiness, and to the final operational deployments and war fighting. The defence of western democracy relies primarily on a complex interconnected system of physical critical infrastructure. Both individually and collectively, it constitutes the primary targets for aggressive states and terrorists, so it must be protected not only from view but also from fire.

4. Critical Infrastructure Definition and Deployment

Critical Infrastructure has been categorised differently in almost every country and international partnership (EU, NATO, Critical 5) that recognises its strategic importance. This may appear disjointed at first but the salient sectors have been identified and included across most if not all relevant national and international frameworks, demonstrating an underpinning joined-up acceptance of their fundamental critical nature.

This “skin deep” acceptance, however, could be described as only the tip of the iceberg. It is only when drilling down into the operational and tactical elements of each sector and segment that the taxonomic picture becomes clearer, demonstrating not only the interconnectedness of our critical infrastructure sectors, but also the gaps between threat definition and the deployment of a proactive (whether passive or active) response.

5. A Sovereign Perspective and Critical 5

The Critical 5 is a forum within the Five Eyes intelligence-sharing network (Australia, Canada, New Zealand, the United Kingdom, and the United States). The aim of the forum, which was established in 2012, is to strengthen cooperation between the Five Eyes states and enhance their ability to address threats to critical infrastructure.

Critical 5 nations have agreed that to meet the challenges of both current and future threats to critical infrastructure they must:

- Modernise policies
- Review the definition of critical infrastructure and sector composition
- Develop stronger information sharing tools and partnership mechanisms

In response, individual nation states have developed (or are in the process of developing) more detailed national criteria and frameworks relating to their individual security situations.

5a. The United Kingdom:

The United Kingdom has 14 identified critical infrastructure sectors, each one falling under a relevant government department for purposes of coordination and management:

- Chemicals
- Civil Nuclear
- Communications
- Defence
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water
- Data Centres (added Sept 2024)

In 2018, the United Kingdom developed the dedicated Criticalities Process to identify and define critical infrastructure assets and their supporting systems. This process is

now supported by the Critical National Infrastructure (CNI) Knowledge Base platform allowing for a visualisation of critical national infrastructure data, highlighting interdependencies and relationships between assets to understand potential cascading impacts of risk.

The UK National Protective Security Authority (NPSA) states in its open-source document, “Improving our Understanding of Critical Infrastructure” that the CNI Knowledge Base is the “single source of truth for the UK CNI, enabling government analysis to visualise the criticalities data”. This statement raises questions on the accuracy of relying on a “single source of truth” and the fundamental challenges of analysing and cross-referencing single source data. In the same document the criticalities process is defined as:

“...giving risk owners in government (i.e. each sector’s Lead Government Department) a common approach to collect and structure data on the CNI they are responsible for. The process supports the systematic identification of the essential functions, the systems that provide them (and their interdependencies), and the organisations that operate those systems. This information is tied to the impacts that a system’s failure would have (both within and across sectors).

- **Step 1 - Map essential functions:** Understanding what is important.
- **Step 2 - Determine systems mapping:** Identification of the systems that provide the function.
- **Step 3 - Assess sector impacts:** Understanding the impact of system compromise.
- **Step 4 - Identify supporting systems, organisations and relationships:** Mapping the systems in more detail.
- **Step 5 - Assess cross-sector impacts:** Understanding the impact on other sectors.”

Further drilling down into the critical infrastructure landscape, the UK Government published the Resilience Framework in December 2022, focusing on the foundational building blocks of resilience, through better prevention, mitigation, response to and recovery from the risks the nation faces. The United Kingdom Government has committed to introducing CNI standards by 2030, which might arguably appear a little late at the time of writing. This is exemplified in the 2023 Resilience Framework Update

(published on 4 December 2023) which set out three core principles to underpin a strategic or fundamental approach to resilience:

- *A developed and shared understanding of the civil contingencies risks we face is fundamental.*
- *Prevention rather than cure wherever possible: a greater emphasis on preparation and prevention; and*
- *Resilience is a ‘whole of society’ endeavour, so we must be more transparent and empower everyone to contribute.*

One of the challenges in facilitating such an open-source approach is that the CNI Knowledge Base and its data are held in a secure environment and accessed only by appropriately cleared government officials. Despite these security constraints the NPSA are evolving rapidly alongside their Critical 5 partners, embracing critical infrastructure security month and developing new protective cyber and physical measures for public consumption. The main challenge, however, is that the physical threats, like the cyber threats are constantly changing shape moving from, low level criminal activity, to marauding terrorist attack, deniable sabotage (undeclared warfare) and ultimately open hostilities (declared warfare).

5b. The United States:

The US National Security Memorandum 22 on Critical Infrastructure and Resilience defines critical infrastructure as that which “comprises the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety”. It further states that critical infrastructure “....is diverse and complex, and includes distributed networks, varied organizational structures, operating models, interdependent systems, and governance constructs.”

In the United States, critical infrastructure security is coordinated by the Cybersecurity Infrastructure Security Agency (CISA) and built on a partnership between government and private industry, a vital collaboration when implementing policy to manage nationally related risk. Like all western democracies, it is important to highlight that both public and private entities own and operate the nation’s critical infrastructure.

This is reflected in NSM 22 which states that that “The Secretary of Homeland Security shall develop and submit to the President on a recurring basis every 2 years a National Infrastructure Risk Management Plan (National Plan), which shall be informed by: (1)

individual sector-specific risk assessments and risk management plans; and (2) a cross-sector risk assessment.”

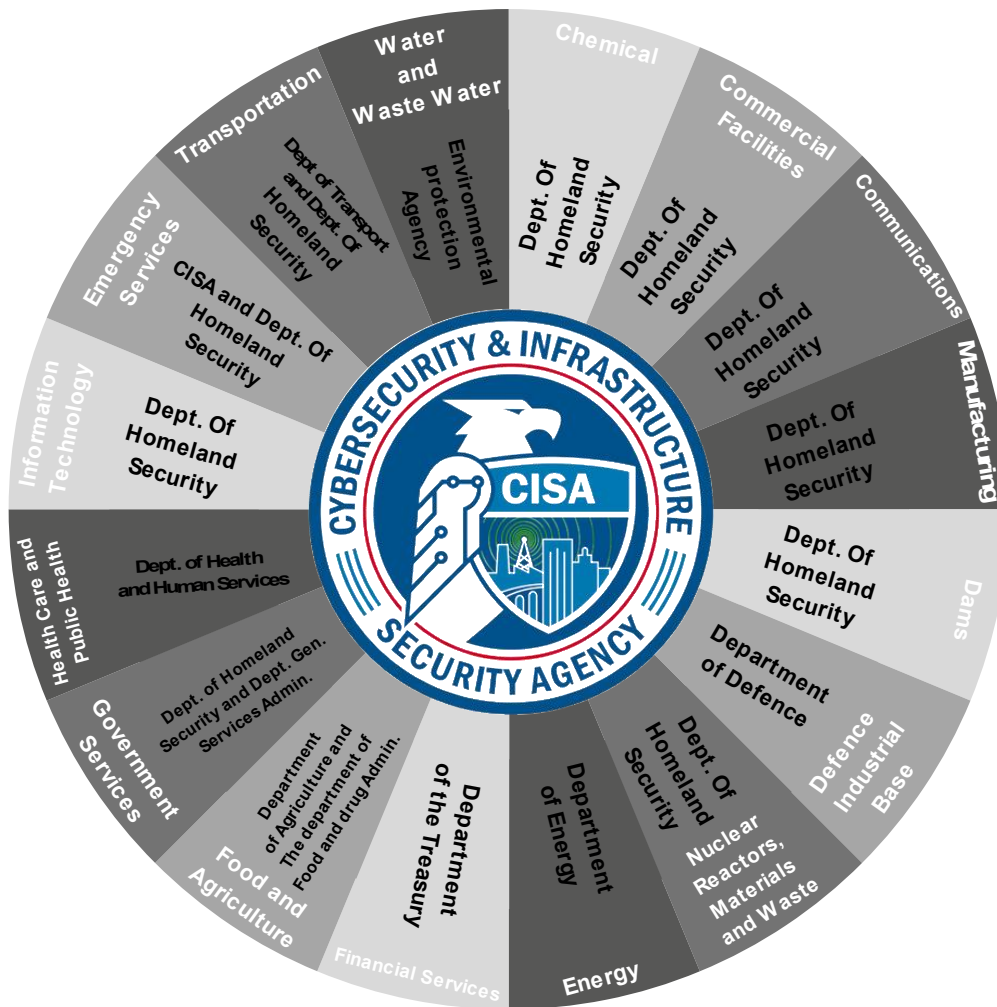
As highlighted in Fig. 2, the responsibility for delivering the policy goals of NSM 22 is distributed across multiple federal departments, performing as “Sector Risk Management Agencies (SRMA).” Each of the 16 critical infrastructure sectors have a designated SRMA with authorities, expertise, and capability aligned to that sector. In addition, NSM 22 introduces the concept of Systemically Important Entities (SIEs), acknowledging that specific organizations and systems have far-reaching impacts that extend beyond their immediate sectors.

This existing national infrastructure security framework provides a collaborative partnership model inclusive of programmes for consolidating information and expertise from government and industry. Like the other Critical 5 nations activities these programmes include awareness and outreach campaigns like the annual Cybersecurity Awareness Month, the annual Critical Infrastructure Security and Resilience Month, and broader national awareness programmes that offer partner toolkits. These programmes allow for sharing substantive information across the private sector and with state, local, tribal, and territorial governments.

This high-level stance stands out in the Critical Infrastructure space and the United States should be praised for their detailed approach to critical infrastructure protection. Notably, the Cybersecurity Infrastructure Security Agency (CISA), is proactive in fostering relationships with international partners to promote collaborative information sharing, cyber security best practices, and partnership models across the globe, as it is recognised that cyber and physical security threat actors are not constrained by geographic boundaries.

Fig. 2: The 16 US Critical Infrastructure sectors and the Sector Risk Management Agencies (SRMA) which are responsible for their coordination, management and reporting to the national Cyber Security Infrastructure Security Agency (CISA).

Source data from CISA.



6. Critical Infrastructure Threat Response - Analysis

Analysis of the threat responses at the international and national levels indicates that, when addressing the threats to critical infrastructure, a traditional three-tier approach is emerging. Interestingly, despite the US and UK aligning at the strategic and operational levels, their approaches differ at the tactical level.

Strategic – Critical Infrastructure Sector identification and classification at the national level through a designated national government agency.

Operational – Segmentation of Critical Infrastructure and Key Resources (CIKR) Sectors – Segment threat identification and planning: detail, data, R&D, mapping and partnerships.

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for the coordination and collation of all 16 sector-specific plans and ensures that they dovetail into the National Infrastructure Protection Plan (NIPP) risk management framework. In turn, 16 designated Sector Risk Management Agencies

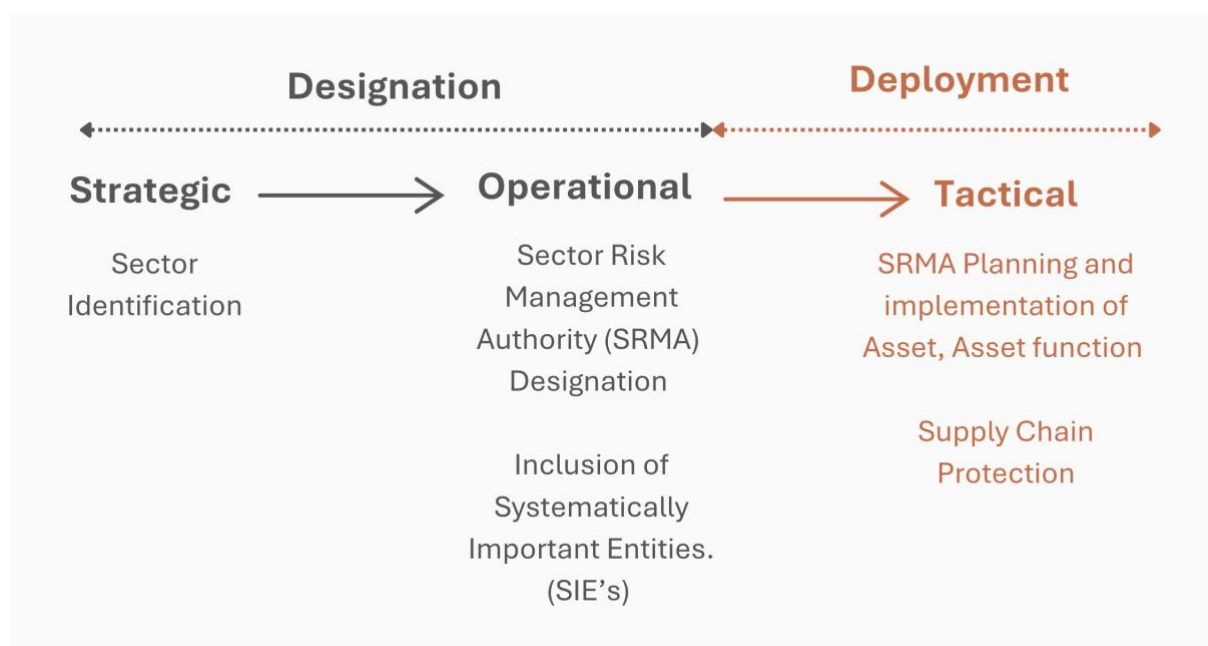
(SRMA) which are responsible for these plans then develop sector-specific plans through a coordinated effort in conjunction with their public and private sector partners. As an example, the Department of Defense is designated as the Sector Risk Management Agency (SRMA) for the Defense Industrial Base Sector.

In the United Kingdom, a similar structure exists at the operational level, funnelling and managing data through a single data platform under the responsibility of the National Protective Security Authority (NPSA), an office of the Security Service, MI5. However, as detailed above, notable differences arise at the tactical level.

Tactical – Implementation – Deployment of Critical Infrastructure and Key Resources (CIKR) **asset and supply chain physical and cyber protection**, relevant to threat. The tactical level is where the “rubber meets the road”, providing tangible protection against both cyber and physical attack and mitigating the non-confrontational threats of adverse weather and structural decline. See Fig. 3 for the Critical Infrastructure direction of travel.

Fig. 3: Critical Infrastructure Protection - Direction of Travel

Based on the US Cybersecurity and Infrastructure Security Agency Model and National Security Mandate 22



7. Identified Threat Vectors

Two primary attack vectors emerge from analysing the threats to critical infrastructure, the physical-attack vector (including physical accidents) and the cyber-attack vector. In

turn, non-confrontational threats come in the form of adverse weather conditions and structural decline.

Only when drilling further down into the “Critical Infrastructure Prism” (introduced later in Fig. 4) can we identify how these threats are best addressed, specifically within the two attack vectors where threats are aggressively deployed. These threats are based on their potential for interrupting, disabling, disrupting, or destroying our capacity to operate as a society or defend our sovereignty. Analysis and acceptance of how we, as western democracies, are to be attacked is strategically essential; however, dialogue, acceptance and designation of threats falls short of delivering a physical deterrent or mitigating a threat.

When defined in a Strategic, Operational and Tactical prism, we can see that it is at the Tactical level where, in much the same way as it is in conventional conflict, change is tangibly engineered and threat mitigation tangibly deployed. This becomes of great relevance when physical threats increase and converge, and existing levels of protection are no longer fit for purpose.

7a. The Critical Infrastructure Threat Prism (CITP) demonstrates how we can view critical infrastructure threats across all three levels and the importance of the tactical level in a real-world survivability context.

This is highlighted in Fig. 4 and, in addition to showing the separation of threat responses, via the grey arrows demonstrates the complex convergence of threats – with the yellow arrow highlighting the migration benefit of Physical Attack Vector threat mitigation measures into the two non-confrontational threat vectors.

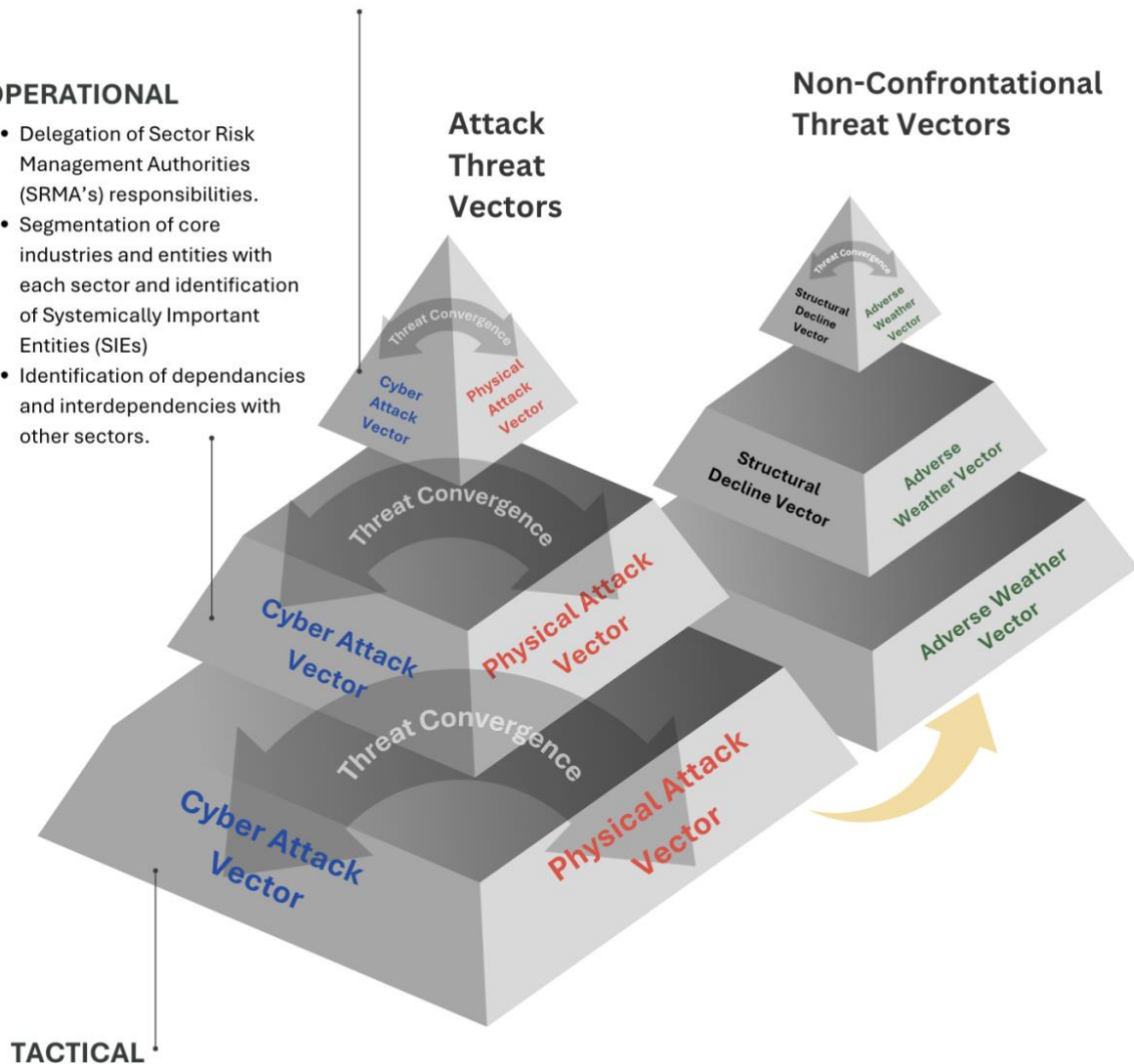
Fig. 4: Critical Infrastructure Threat Prisms

STRATEGIC

- National / International Threat recognition
- Classification of national Critical Infrastructure sectors.
- Inclusion into a national threat assessment.

OPERATIONAL

- Delegation of Sector Risk Management Authorities (SRMA's) responsibilities.
- Segmentation of core industries and entities with each sector and identification of Systemically Important Entities (SIEs)
- Identification of dependencies and interdependencies with other sectors.



TACTICAL

Development and deployment of Critical Sector Specific Plan:

- Physical. Critical Asset identification - Conducted by the SRMA's
- Physical. Asset threat analysis - Conducted by the SRMA's and the SIE's (Introduction of Levels 1,2,3)
- Physical. Asset threat mitigation - Implementation of Protective Response conducted by SRMA's, SIE's and other private sector entities
- Cyber. Critical Asset identification - Conducted by the SRMA's
- Cyber. Threat analysis - Conducted by the SRMA's, SIE's and other private sector entities.
- Cyber. Asset threat mitigation - Adoption of Minimum Security and Resilience Requirements, implementation of Secure by Demand. 12 identified considerations for operational technology owners and operators
- Adverse Weather. Asset threat identification - Conducted by the SRMA's
- Adverse Weather. Asset threat analysis. - Conducted by the SRMA's and the SIE's
- Adverse Weather. Asset threat mitigation. - Implementation of Protective Response conducted by SRMA's, SIE's and other private sector entities
- Structural Decline. Asset threat identification. - Conducted by the SRMA's
- Structural Decline. Asset threat analysis. - Conducted by the SRMA's and the SIE's
- Structural Decline. Asset threat mitigation. - Implementation of Protective Response conducted by SRMA's, SIE's and other private sector entities

7b. The Cyber Attack Vector

State actors and commercial entities have faced tech-based attacks since the early 1980s. However, the cyberTAP service at Purdue University have noted that historically, the first cyber-attack occurred in 1834, well before the internet was even invented. Attackers stole financial market information by accessing the French telegraph system.

Today the situation has evolved dramatically with an entire ecosystem of criminal organisations deployed incognito. Add nation-state actors to the mix alongside individual hackers targeting specific organisations, and you have an attack vector able to significantly impact the function of critical infrastructure, requiring a proactive rather than reactive defence response.

The Centre for Strategic and International Studies (CSIS) have catalogued significant cyber-attacks since 2006. They report that in November 2024, the United Kingdom's National Cyber Security Centre (NCSC) found a three-fold increase in the most significant cyberattacks compared to the previous year, highlighting the scale of this threat. The NCSC provided support in that short period for 430 cyberattacks, 89 of which were “nationally significant” and listed China, Russia, Iran, and North Korea as “real and enduring threats”.

CSIS also reported that same month that hackers – attributed to China, dubbed Salt Typhoon – breached at least eight U.S. telecommunications providers, as well as telecom providers in more than twenty other countries, as part of a wide-ranging espionage and intelligence collection campaign targeting the critical infrastructure designated communications sector. Illustrating the scale of the challenge posed, researchers believe the attack began up to two years prior and still infects telecom networks to this day. Attackers stole customer call data and law enforcement surveillance request data and compromised private communications of individuals involved in government or political activity. CSIS also reported that, in November 2024, Chinese spies planted a chip in a former U.S. three-star general's conference name tag to track his every move during his time serving in the Indo-Pacific, highlighting that cyber-attacks also have a physical espionage element.

The evolution of the cyber threat has resulted in escalating security expenditure. Statista.com have stated that their global indicator – Estimated Cost of Cybercrime – in the cybersecurity market has forecast costs to continuously increase between 2024 and 2029 to US\$ 6.4 trillion (a 69.41% increase). It predicts that after an eleventh consecutively increasing year, the indicator will reach an estimated US\$ 15.63 trillion.

Organisations are urged to adopt proactive security measures to mitigate operational impacts, particularly as AI technologies and IoT devices expand.

Such predictions have driven the Cybersecurity and Infrastructure Security Agency (CISA) of the United States, joined by 11 domestic and international partners, including the European Commission, published on January 13th, 2025, a document providing details on how Operational Technology (OT) owners and operators should integrate security into their procurement processes. The report entitled: “Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products”, **recommended the inclusion of 12 essential security elements into all official and corporate OT procurement. By doing so, critical infrastructure organizations can enhance the mitigation of cyber threats and transition away from outdated systems.**

Discussing this report, Grant Geyer, chief strategy officer at platform developers Claroty, stated that “by creating a clear set of security requirements, CISA’s Secure by Demand guide for OT provides the opportunity to create a groundswell of market-driven demand for uniform security standards and needs from automation manufacturers. This dynamic should force a mindset shift that the imperative is not a false notion of prioritizing functionality or security – the requirement is secure functionality.”

He added, “some asset owners and industry professionals will correctly argue that any efforts started today by a manufacturer won’t have a positive impact for years given the long build cycles and technology obsolescence period of industrial control systems (ICS). To this I’d say, while the best day to plant a tree was twenty years ago, the second-best day to plant one is today.”

The report also stated that:

“By ensuring the deployment of secure products on their networks, critical infrastructure owners and operators can reduce the potential damage from cyber threats and protect their systems from exploitation. Making these systems resilient is essential for maintaining public trust and the smooth functioning of modern societies. Also, buyers should look for manufacturers that demonstrate their adoption of Secure by Design and International Society of Automation (ISA) 62443 standards.”

For the purposes of this paper, we can use a simple three-stage analysis approach. Focusing on the western democracies we can broadly observe the Cyber Attack Vector threat situation (arguably more advanced than the Physical) as comprising of:

- **Threat Identification** – The threats have been identified, and the vector undergoes a proactive and dynamic updating process.
- **Threat Acceptance** – The threat levels have been accepted by all relevant agencies.
- **Threat Intervention** – Rapid response providing both continued threat surveillance and analysis and the development of credible online deterrence.

7c. The Physical Attack Vector

Physical attacks against critical infrastructure have been an element of warfare since the days of laying siege to castles and poisoning wells. The objective then, as today was to disrupt, disable or destroy an adversary's ability to function and defend themselves. The physical attack incorporates a violent approach that unlike its cyber co-threat arguably has a more direct and in many cases immediate effect on human life and psychology, as well as operability.

A wide range of Kinetic Energy (KE) threats exist against critical infrastructure. However, effective defence will only be possible if there is an understanding of the physical nature of likely challenges. Such threats range from those that non-state actors can access (small arms, improvised devices) through to more sophisticated systems such as Man Portable Air Defence Systems (MANPADS) for larger organisations, along with those which are purely the domain of state actors (for example, multi-hundred-pound mass air launched munitions). The physics

underpinning such systems operates across three core (but overlapping) regimes as shown in Figure 5.

Fig. 5: The nominal physical (velocity) threat regimes against critical infrastructure.

Increasing velocity / strain-rate; governing physics moves from strength-of-material analysis through to hydrodynamics / shock-wave analysis.



Ballistic (low-velocity Kinetic Energy (KE) up to ca. 1.2 km/s.



- Low KE effective (small arms) through higher velocity threats (rifle rounds). Hardening cores enhance Kinetic Energy Density (KED), enhancing target perforation.
- Protection approaches typically passive - high density armour systems.
- **Threats are relatively straight forward to mitigate at scale for built infrastructure.**



Quasi-hydrodynamic (high-velocity kinetic energy (KE), typically 1.2-3 km/s).



- Intermediate velocities; targets / projectiles begin to exhibit hydrodynamic-like characteristics. Kinetic Energy Density (KED) fundamental requires high density armour.
- Effectors / weapon systems include artillery rounds Explosively Formed Projectiles (EFP's) and high-velocity fragments.
- **Such threats to Critical Infrastructure (CI) are predominantly land based or secondary (fragments from a detonating air-launched weapon).**



Hydrodynamic / shock-driven (>3 km/s):

- Very high resultant pressures - strain rates that overcome material shear strength establishing shockwaves.
- **Penetrators:** Shape Charges (SC's) / High Explosives Anti-Tank (HEAT): multiple scale from Rocket Propelled Grenade (RPG) to Storm Shadow air launched cruise missile, where penetration is many times the diameter of the charge entering reinforced structures.
- **Explosive Systems (bombs):** detonation - a chemically supported shockwave sharing the physics of hydrodynamic systems. Surface driven systems High Explosive Squashed Head (HESH) generating effects remote from the point of impact. Alternatively, Bombs Royal Ordnance Augmented Charge (BROACH) create massive localised overpressure that disrupt targets. Vehicle borne Improvised Explosive Devices (VBIED's) and attack UAVs (drones) can also significantly impact CI targets but at less financial cost.
- **Significant CI threats. Protection is challenging requiring up-armouring and increased resilience of built infrastructure (similar to that on vehicles). Novel approaches are required with specific attention to behind - armour effects.**

Even behind friendly lines, critical infrastructure is vulnerable across the whole range of threats. On the ground, distance and architecture can help mitigate the potential effects of systems such as Vehicle-borne Improvised Explosive Devices (VB-IEDs). However, the importance of protecting against air-based systems becomes clear in the current environment where even small-scale actors can deploy drone-based or even small-scale missile systems (e.g. the on-going terror threat to the state of Israel in the Middle East). Such emerging low-tech threats are particularly relevant to infrastructure such as data centres where the majority of security is based on human access control. Attack drones are now easily configured from off-the shelf units and capable of creating explosive access for second-wave drones to remotely target specific internal areas.

At the top end of the scale, penetrating threats (such as ‘bunker busters’) are available to almost all potential adversaries. Importantly, critical infrastructure protection does not currently consider the same.

As suggested above, aggressive physical threats against critical infrastructure can be deployed through a plethora of complex and hybrid forms of attack. Critical infrastructure can be targeted by terrorists/extremists, armed civilian groups, revolutionaries, specialists in unconventional warfare, state actors from a hybrid undeclared covert perspective, state actors in an undeclared overt perspective or when war is openly declared.

Because of the hybrid nature of threats to critical infrastructure, including military attacks against civilian targets, its security is that of an “all of society” responsibility and cannot be defined in the separate conventional military or civilian dimensions.

It’s important to highlight that a high percentage of critical infrastructure targets are co-located within or close to human centres. This situation has been intensified with the development of smart cities providing an aggressor with a three-pronged potential outcome: i) destruction of the asset, ii) a cascading effect on other critical infrastructure assets, and iii) the incitement of fear across the human terrain.

In many cases, human fear and disillusionment can provide a more destructive long-term outcome for an attacker than simply disabling or destroying a primary target. This potential impact is further amplified in a lightly protected or ill-prepared built environment where the populace will consequently feel that their well-being, security and the protection of their essential assets have not been valued highly enough to warrant physical hardening.

These multi-layered physical and psychological threats relate directly to the UK's 2023 Resilience Framework Update (published on 4 December 2023) and its three core principles to underpin a strategic or fundamental approach to resilience, highlighted previously in this document, the focus being on a shared understanding of civil contingencies and a **prevention rather than cure mindset** from a “whole of society” perspective.

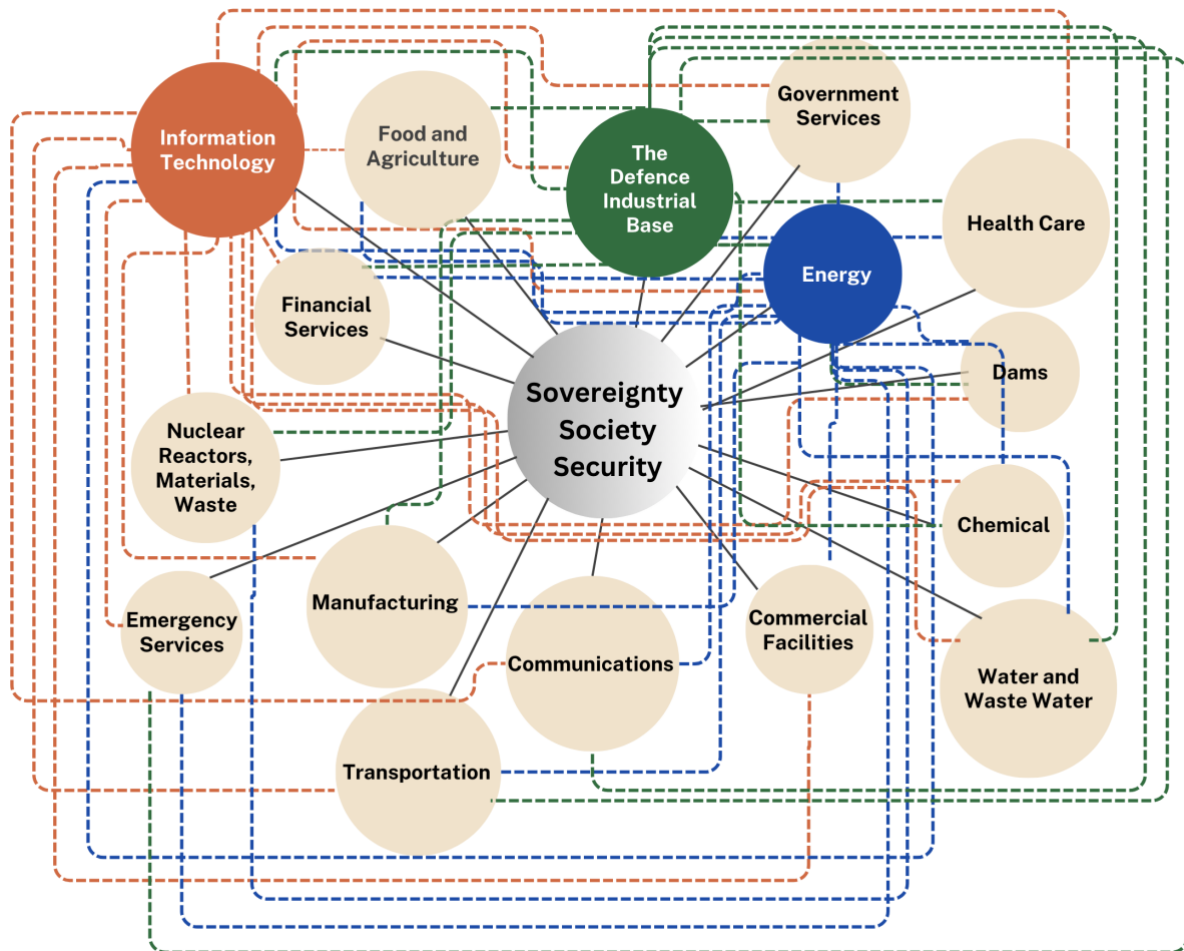
The Second World War demonstrated a turning point in global human conflict as towns and cities became strategic targets and, in many cases, urban battlefields – primarily due to critical infrastructure being amassed in and around the urban centres of human population, industrial production and the centres of power. With the increased urbanisation of our societies and the interconnectivity of our critical infrastructure, incorporating physical resilience into its relevant built environment is more important now than ever before.

8. Critical Infrastructure Interdependence (CII) and Threat Realization

Figure 6 highlights the complexity of Critical Infrastructure Interdependency (CII) using only three of its sixteen recognised sectors (US model – Fig. 1). This illustration demonstrates not only a physical resemblance to an electrical circuit diagram, it also shares an operational one as it may take only a single significant “short” to disable the entire circuit. That “circuit” relates to our ability as a community or nation to operate at a 21st century capacity and defend our sovereignty against 21st century threats.

The reality is that because of our interoperability and interdependence, we could be in a position whereby one targeted attack (low or high-tech) could be responsible for a complete breakdown in our societal function or prevent our ability to govern.

Fig. 6: Illustration of the interdependency between Critical Infrastructure assets.



9. Owning and Influencing the Defence Space

The physical attack vector, like its cyber cousin, requires a proactive response. In conflict and high-risk areas, where the potential of attack is possible or probable, defence against attack is usually deployed in a layered or in-depth fashion, dictated by relevant and evolving threats. Responses may range from or be a combination of early neutralisation of identified aggressive forces, on (or below) land, sea, or air, the use of Electronic Warfare (EW) to disable guidance, communication or arming systems, and inflight neutralisation using air assets or a surface-to-air capability. These responses are essential despite requiring constant operational surveillance and the ability to deploy geo-relevant, costly, technical and human assets at short notice. In the case of air attacks the sovereignty of third-party airspaces may also be a consideration and the possibility of regional conflict escalation. Such kinetic approaches are, however, difficult to sustain in the long-term. They are also far from effective especially against low-tech kinetic attack.

As an example of the evolving nature of challenges – making active defence so complex – aerial glide bombs developed using “dumb bombs” sourced from huge Soviet era stockpiles have become one of the greatest threats to Ukrainian civilians in cities, a point highlighted in January 2025 by Danielle Bell, head of the UN Human Rights Monitoring Mission in Ukraine (HRMMU). She also stated that they are one of the main reasons why the number of killed and injured in 2024 increased by 30 per cent compared with 2023. According to HRMMU figures, Russian glide bombs killed 360 Ukrainian civilians in 2024, and injured 1,861, a threefold increase in fatalities, and a sixfold increase in injuries compared to 2023. The destruction of infrastructure also demonstrated a consummately significant increase.

It is of course on the ground where detonation usually occurs and where the Passive Ground Defence (PGD) element provides the last opportunity for a defender to “own” its defence and mitigate the impact of an attack. Effective PGD strategies provide a defender with the ability to limit the devastation of an attack, reduce catastrophic consequence, protect critical assets, maintain operability and save lives, taking back ownership and denying an attacker significant situational influence. Importantly, as physical threat vectors are – ultimately – limited, such approaches have the potential to mitigate the need for the constant evolution that accompanies the active domain.

The primary PGD response to an aggressive kinetic threat is to increase the resilience of the built environment, in particular those buildings/structures that house or constitute defence assets, critical infrastructure and support the protection of life, directly and indirectly.

Unlike the important aggressive forms of defence deployed in the layered or in-depth approach, PGD - or the hardening of the built environment - is a cost effective, minimal maintenance, site adaptive, permanent defence asset that also demonstrates a morale boosting active commitment to protect life across the human terrain. In an idealised situation, it would be similar to an airbag in a car, in that it is unnoticeable but vital when you need it.

Unfortunately, investment into the PGD of Critical Infrastructure, defence assets and social facilities has been negligible across NATO countries and their allies since the fall of the Soviet Union. This defence underreach is apparent despite existing and emerging threats that dictate a growing need.

Once again, using a three-stage approach to analysis, we can observe the broad Physical Attack Vector threat situation – however, unlike the Cyber Vector, the chain is incomplete:

- **Threat Identification** – The threats have been identified; the vector is undergoing reassessment in light of changing geopolitical threats and the capabilities of potential aggressors.
- **Threat Acceptance** – The threat potential has been accepted by all relevant agencies **yet in some cases probabilities and the consequences may not be accepted until they become a reality.**
- **Threat Intervention** – **Physical interventions to enhance survivability do not align with identified threats.**

There are detailed national frameworks, recommendations and hardware for enhancing domestic security in homes, offices and other built structures against criminal activity. There is legislation and classification relating to identifying key critical national assets, yet little physical protection deployed to increase their survivability, ***from a prevent rather than cure mindset.***

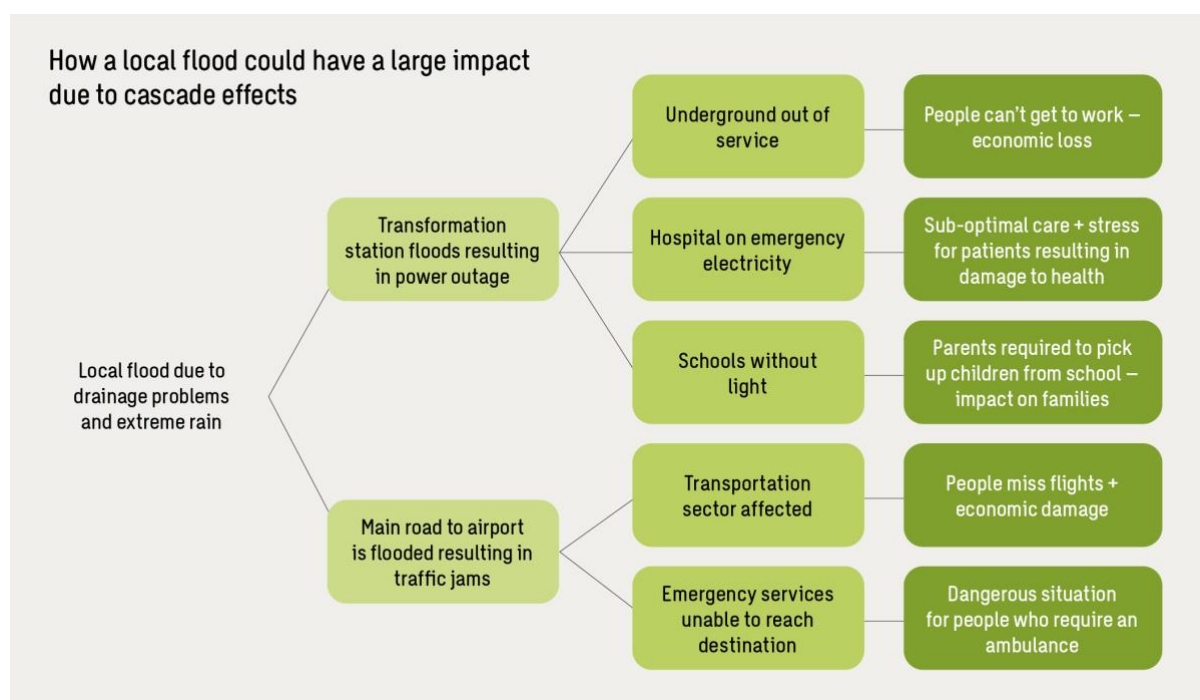
With this in mind the question can be posed as to whether it is time that a similar approach be developed and deployed within the physical attack vector as in the cyber-attack vector – e.g. **should there be a minimum resilience security standard for physical critical infrastructure?**

10. Non-Confrontational Threats – Adverse weather and structural decay

While not the main focus of this discussion, there are clear potential benefits in exploring the reinforcement (and replacement) of infrastructure in terms of managing the consequences of adverse weather that have been linked at the epistemic scientific community level to the warming of the planet.

The term adverse weather refers to weather that is a potential threat to life and property or causing disruption of normal day to day activities and long-term productivity and stability. Such events can include heat waves, freezes, heavy rain, tornadoes, tropical cyclones and floods of which the consequences can, and have been catastrophic. In the past, adverse weather events have led to the destruction of critical infrastructure and a breakdown of essential services such as water, power/energy, transport, communications, health and emergency services. Such breakdowns have huge consequences – potentially greater than those of human-induced conflict – resulting in and adding to the cascading effects of famine, disease, mass human migration, conflict, productivity and in some cases even the ability to govern. The chain reaction of such cascading effects in a western rural landscape has been the subject of research by the architectural design company SWECO as seen in Fig. 7, demonstrating how a simple drainage problem can lead to broad economic loss and, in extreme cases, loss of life.

Fig. 7: Cascading effects of localised failure.



Source. Urban Insight Report by SWECO Ltd – Expect the Unexpected, Floods and Critical Infrastructure

The financial cost of adverse weather adds to its catastrophic effects, something highlighted by a report commissioned in 2024 by the International Chamber of Commerce which estimates that climate-related extreme weather events have cost the global economy more than \$2 trillion over the past decade. In addition to the financial cost, SWECO state that, “What stands out is that the human impact of any failure of critical infrastructure, including emotional damage, is often not given enough attention in policy documents and is sometimes completely overlooked. In addition to rebuilding homes and infrastructure, attention to mental resilience is essential for the proper functioning of a city.”

Add crumbling infrastructure to the threats from adverse weather and the situation increases in severity. In the UK and US, many critical structures were built during the post-war boom years and have now exceeded their designed lifespans. The reinforced concrete used at the time are not as enduring as first presumed. Some problems incurred today include:

- **Concrete Spalling**, flaking or chipping of the surface layer, often caused by freeze-thaw cycles or the use of de-icing salts.
- **Corrosion of Reinforcement**, when the steel reinforcement inside the concrete begins to rust, it expands and causes the surrounding concrete to crack.

- **Alkali-Silica Reaction**, a chemical reaction between the alkali in cement and the silica found in aggregates; this reaction can lead to swelling and cracking.
- **Salt-laden air** in coastal regions and the freeze-thaw cycles in colder areas are environmental factors that can adversely affect concrete structures.

The 21st century has provided the engineering and construction industry with new and emerging challenges, particularly when ensuring the survivability of public buildings and critical infrastructure. The adverse weather and the degradation of built environments across western democracies have become a seminal issue; architects, engineers, scientists, government officials and the general public have voiced their concerns in light of recent alarming failures. It is apparent that new thinking and new materials are required to ensure built environments can withstand new levels of impact, erosion, wear and tear, if they are to be cost effective and fit for purpose throughout their life cycles.

Subjecting the non-confrontational vectors of the Critical Infrastructure Threat Prism, Adverse Weather and Structural Decay to the same simple form of analysis as the two attack vectors, Physical and Cyber, we arrive at the following:

- **Identification** – Many threats have not only been identified but experienced.
- **Acceptance** – The threat levels have been accepted by all relevant agencies and widespread concern aired across the broader human terrain.
- **Intervention** – Due to the enormity of the threat, physical interventions to enhance survivability against adverse weather and structural decline have been implemented; however, not at pace or scale relevant to the threat.

11. Threat Convergence

“Human evolution has placed the world of linear threats and security silos into the history books.”

Throughout this paper, we have analysed and explored each one of the critical infrastructure threat vectors and observed gaps in how we address them. In addition, we have highlighted the ultra-interconnectivity of western societies and how this has increased rather than reduced our sovereign fragility. This fragility is further enhanced through exposing our critical infrastructure to not only the threats of a single vector failure but to the far more catastrophic and probable scenario of destructive hybrid threats, whether malicious, non-confrontational or a combination of both.

The nationally important value chains within the Defence Industrial Base, Manufacturing, Food/Agriculture and Energy sectors are particularly susceptible to the catastrophic effects of a hybrid cyber/physical compromise through the disruption or destruction of their critical infrastructure assets.

Threat convergence or hybrid threats to critical infrastructure bring together the different threat vectors in various configurations, forming a multi-level threat picture that has the potential to create a poly-crisis. The threat of poly-crisis is very real, requiring an equally multi-layered and proactive response able to future-proof the normality of our societal landscapes and defence capabilities.

As an example, a hybrid assault on the components of a digital system may include causing the physical destruction or disabling of its power source, connectivity, or network infrastructure, providing hackers with a window to access systems and install malware to conduct data theft or manipulation.

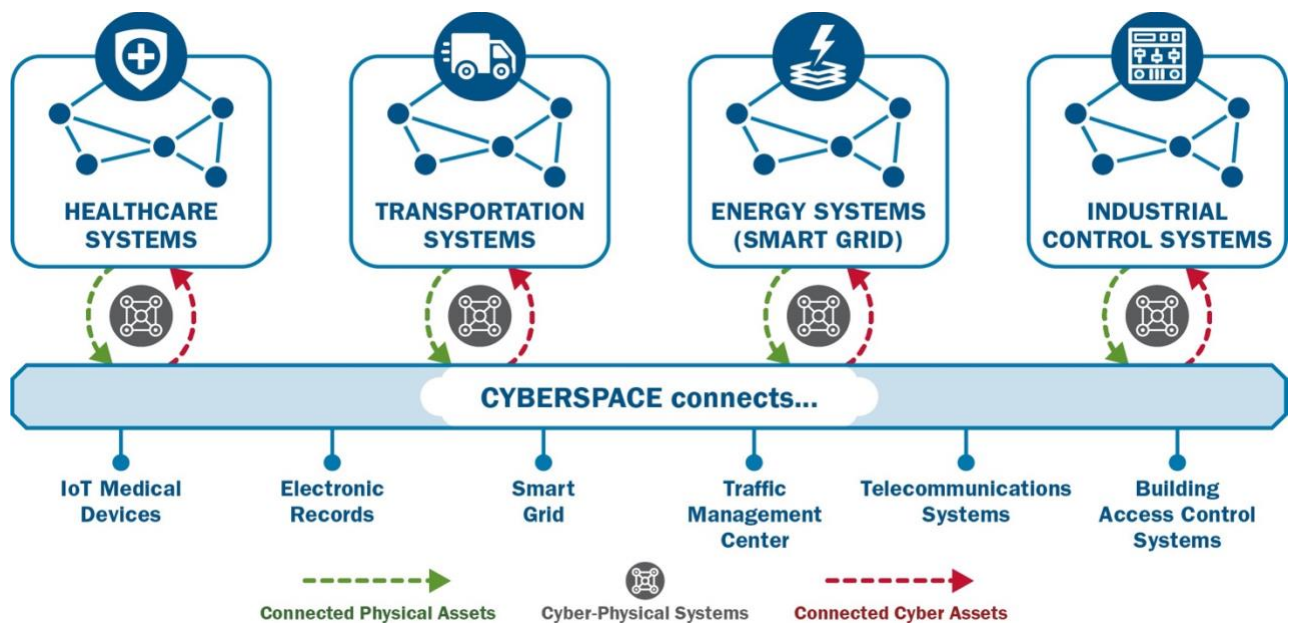
The infrastructure that houses the Internet of Things (IoT) and every one of the identified critical infrastructure sectors is susceptible to physical attack, adverse weather conditions and, albeit to a lesser and more specific degree, structural erosion. It is not a case of if they will be subject to these elements, but when.

The hybrid nature of modern warfare has already facilitated movement from the cyber to the kinetic battlefield.

Such threat convergence is already occurring – for example, the Israeli Defence Force (IDF) claimed that on the 4th May 2019, they partially destroyed a building in Gaza housing an active Hamas cyber warfare hacking unit. The IDF tweeted that, "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed." This is – to the author's knowledge – the first publicly recorded kinetic attack against cyber aggression, demonstrating the active convergence of the cyber and physical domains.

In 2021, the United States Cybersecurity Infrastructure Security Agency (CISA) published its Cyber Security and Physical Security Convergence Action Guide.

Fig. 8: Critical Infrastructure relationships within a Cyber-Physical System (CPS).



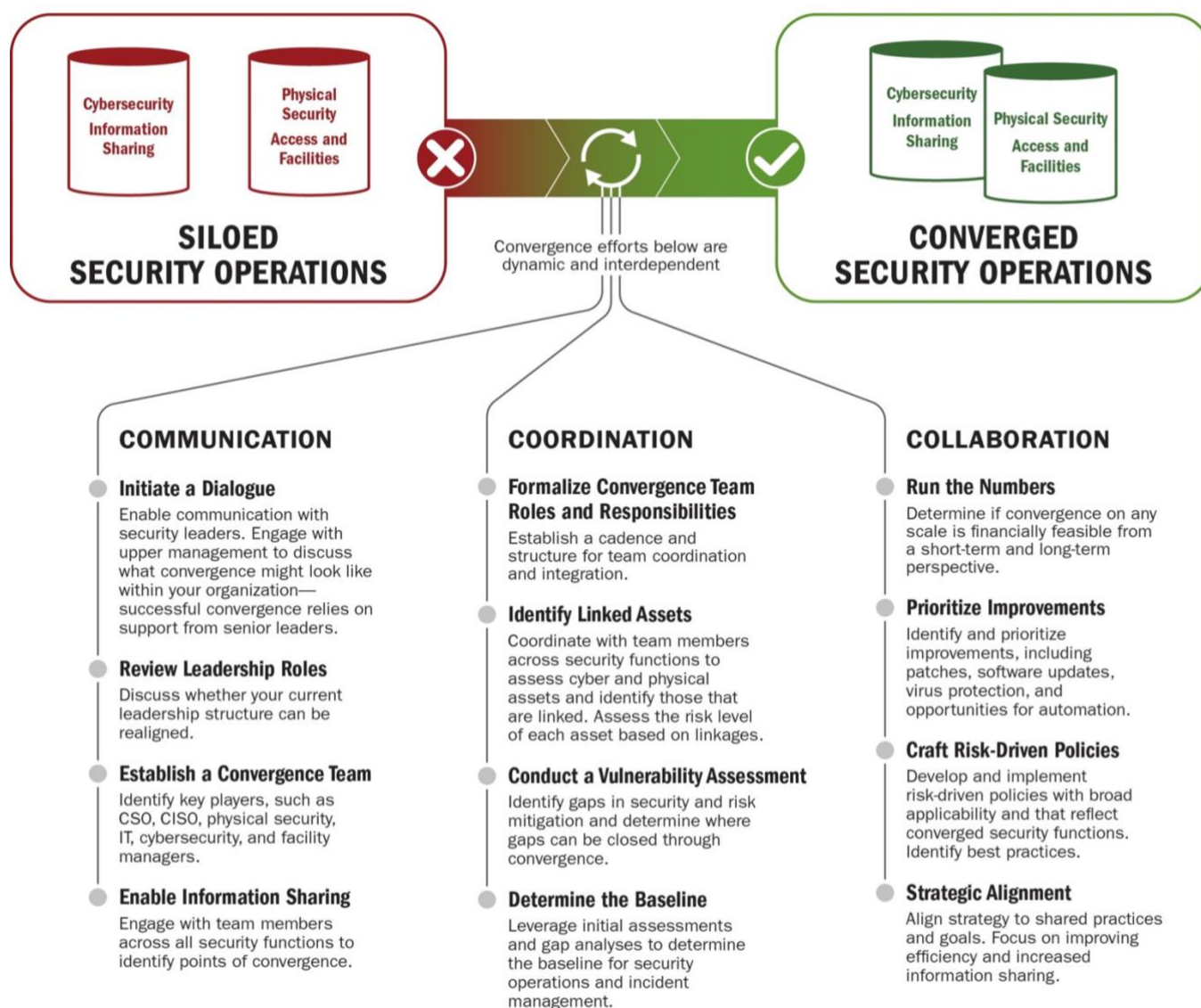
Source – CISA

The Cybersecurity and Infrastructure Security Convergence Action Guide 2021

Fig. 8 is a diagram from the CISA guide demonstrating the Critical Infrastructure relationships within a Cyber-Physical System (CPS), clearly highlighting the potential for the convergence of risk.

In today's world, the evolution of threat and risk is becoming increasingly dynamic. In this area, Fig. 9 highlights the CISA "Framework for Aligning Security Functions" (2021). In light of the findings of this paper and events in Ukraine and Gaza, if such a diagram were to be re-drawn today, we would hope to see the addition of "Implementation" or "Deployment" as a tactical level fourth vertical with the inclusion of enhanced physical resilience to the built environment.

Fig. 9: CISA “Framework for Aligning Security Functions” (2021).

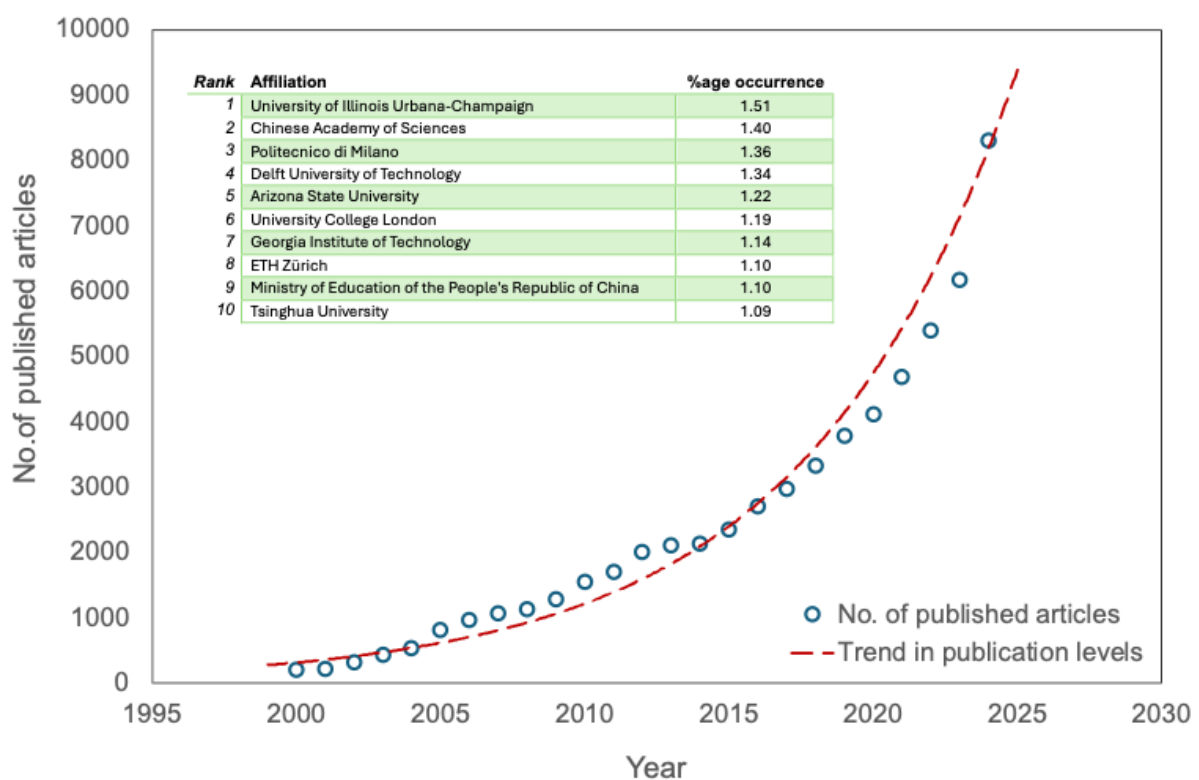


Source: The Cybersecurity and Infrastructure Security Convergence Action Guide 2021

12. Critical Infrastructure Reliance, Destruction and Defence – A Subject of Rapidly Emerging Interest

Work in the Critical Infrastructure defence space is of vital importance across the defence-industrial and academic sectors. However, to date most of the research and development has been very much focused in the former, with protection of Critical Infrastructure only recently coming to the fore in the academic sphere. Fig. 10 effectively draws this out; of particular note is the exponential increase in research activity post-2001, coinciding with the September 11 attacks on the World Trade Centre.

Fig. 10: Trends in publication of peer-reviewed academic papers post-2000 focused on ‘Critical Infrastructure’



Note: across the 2020-2024 period just ca. 60,400 articles have been published in the critical infrastructure arena.

More widely, as shown by the inset table in Fig. 10, while the US continues to lead in research outputs, it is apparent that China is investing at an increasing rate, presumably with a view towards establishing operational overreach.

This emergence of China as a direct intellectual and research competitor to the US / Western sphere should arguably represent a point of concern in the West.

Overall, this development, further reflected in Fig. 11, which highlights the emergence of China as a source of funding, appears to indicate a significantly increased importance being placed on the protection of Critical Infrastructure by China.

Fig. 11: Funding body data for articles explored in Fig. 10.

Rank	Funding body	%age occurrence
1	National Science Foundation	8.48
2	National Natural Science Foundation of China	8.10
3	European Commission	7.54
4	Horizon 2020 Framework Programme	5.02
5	Ministry of Science and Technology of the People's Republic of China	3.48
6	U.S. Department of Energy	2.52
7	Engineering and Physical Sciences Research Council	2.06
8	UK Research and Innovation	2.05
9	Seventh Framework Programme	1.91
10	National Key Research and Development Program of China	1.87

Conversely this enhanced investment from China in research arguably raises the question - do they have a similar interest in Critical Infrastructure from a target acquisition perspective?

The exponential increase in interest highlighted above reinforces the importance of maintaining an R&D edge if the West is to both protect its critical infrastructure assets and also have sufficient understanding to be able to hold at risk, should this be required by those of future potential adversaries.

13.Summary

The interconnected nature of our societies and nations enhances the catastrophic consequences of critical infrastructure failure through attack, decay or natural events by cascading to a level whereby it is difficult to retroactively contain, prompting a proactive or prevention rather than cure strategy. The consequences of cascading critical infrastructure failure have no limit of exploitation and no effective back stop on which we can rely; their destruction has the very real potential to catastrophically affect lives, homes, business, societies, sovereignty, and ultimately freedom.

The title of this paper, “Security by Obscurity is No Defence for Western Survivability”, raises the question – are the western democracies and the defence alliances in an underreaching position concerning the physical defence of critical infrastructure and thereby putting societal and sovereign survivability at risk?

“The mere identification and classification of threat is no substitute for the physical implementation of a credible deterrent and/or defensive action.”

– Ian Saunders. Visiting Fellow Cranfield University, Director Soteria Shielding.



DSPACE

<https://dspace.org/>

Physical Critical Infrastructure Protection - Security by Obscurity is No Defence for Western Survivability

Saunders, Ian; Appleby-Thomas, Gareth J.

2025-04-10

Cranfield University

<https://dspace.lib.cranfield.ac.uk/handle/1826/24093>

Saunders I, Appleby-Thomas G. (2025) Physical Critical Infrastructure Protection - Security by Obscurity is No Defence for Western Survivability. Report, Cranfield University, UK