Understanding the Dynamics of the Cyber Grey Zone: A Conceptual Framework

Shu-Jui Chang, Tim Watson and Iain Phillips
Loughborough University, UK

s.chang@lboro.ac.uk
tim.watson@lboro.ac.uk
i.w.phillips@lboro.ac.uk

Abstract: Cyberspace has become a domain for state and non-state actors to engage in activities that operate in the area between peace and conflict, often referred to as the "grey zone." These activities, which range from legal to illegal, exploit the lack of thresholds and norms, creating challenges for understanding impact and managing consequences. This research examines the complexities of cyberspace and grey zone activities, which operate between peace and wartime, using activities ranging from legality to illegality. Addressing the lack of clarity in understanding their impact and management, the study introduces a five-block framework to systematically analyse and triage these activities. The blocks – i) Incident, ii) Technical Analysis, iii) Strategic Context, iv) Operational Preparation, v) Legality and Political Will. This structured approach enables a comprehensive breakdown of situations, assessing strategic significance and providing a benchmark for evaluating proximity to thresholds. The framework is designed to assist policymakers, strategists, and cybersecurity professionals in navigating the complexities of grey zone activities in cyberspace. This study contributes to developing more effective responses to ambiguous and evolving threats by offering a tool for informed decision-making.

Keywords: Cyberspace, Grey zone, Framework

1. Introduction

Cyberspace has emerged as a transformative domain, reshaping the dynamics of global interaction, conflict, and competition. Unlike traditional domains such as land, sea, air, and space, cyberspace is uniquely intangible, borderless, and evolving. Its pervasive influence has created new forms between peace and war, often called the "grey zone." Grey zone activities are characterised by actions that fall below the threshold of open conflict but exploit ambiguity to achieve strategic objectives (Dobbs et al. 2020, Layton 2022, Maass 2022, O'Rourke 2020). These activities encompass tools, including economic coercion, political pressure, limited military operations, and cyber operations.

For a considerable time, activities in cyberspace were often underappreciated and treated as auxiliary components within the broader grey zone toolkit. However, the growing reliance on cyberspace for critical infrastructure, communication, and governance has highlighted its significance as more than just a subset of grey zone activities. Instead, cyberspace demands independent study and a deeper exploration of its unique characteristics. This research seeks to address this gap by identifying and conceptualising a distinct area of study termed the "Cyber Grey Zone" (CGZ).

Developing effective practices in contested areas requires a robust theoretical foundation to guide understanding and action. Theoretical constructs are not merely academic conveniences but essential tools that shape how phenomena are conceptualised, analysed, and addressed. Frameworks, in particular, provide structured approaches to operationalise ideas and navigate complexity. However, as an academic discipline and formalised research area, the CGZ remains in its infancy. Its foundational agenda has yet to be established, and there is a pressing need to create an overarching framework that defines, describes, and interrelates its constructs. As Krishnan (2009) aptly argues, an academic discipline should have theories and concepts to organise accumulated specialist knowledge.

This research addresses this gap by establishing a foundational benchmark, which identifies its defining characteristics and narratively visualises its structure; the study seeks to explore the landscape of the CGZ within the framework of the Cyber Grey Zone (FCGZ). The FCGZ provides a structured approach to analysing grey zone activities in cyberspace, offering a tool for policymakers, strategists, and researchers to understand better and respond to these complex and evolving challenges

2. Literature Review

2.1 What's the Grey Zone

Grey, much like the colour between black and white, represents a conceptual space within the bipolar framework. The "grey zone" is understood as a space where the engagement between state and non-state

actors occurs (Command 2015), encompassing both military and non-military dimensions (Strachan 2021, Update 2020). It involves a mix of conventional and unconventional techniques (Hoffman 2007, Jordan 2020), operating under both legal and illegal norms (Kiessling 2021, Sari et al. 2024), and straddling the boundary between peace and kinetic warfare (Dobbs et al. 2020, Layton 2022, Maass 2022, O'Rourke 2020).

Other terms are shared, such as Liang & Xiangsui's (1999) proposed unrestricted warfare, and similarly, both NATO and EU favoured the term hybrid threats. According to the NATO (2010),

Hybrid threats are those posed by adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.

As for the EU, the European External Action Service (2018) states that

Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives.

There has been considerable discussion about the nuanced differences among these terms. Still, the central principle here is that they involve escalating tensions by any means, without explicitly breaking the rules, but rather pushing tensions to the edge of potential warfare. Building on these definitions, this study conceptualises the grey zone as a strategic space where actors exploit ambiguity and operate below the threshold of open conflict to achieve political, economic, or military objectives. This definition underscores the importance of understanding the grey zone as a dynamic and multifaceted domain that requires tailored analytical frameworks.

2.2 Cyberspace

Cyberspace, despite being increasingly approached and engaged with every day, remains an area that is not clearly defined. It is often described based on the characteristics of data-centered systems within the global domain, consisting of interconnected communications, information technology, and other systems, networks, and data. This includes dependent and independent systems that process, store, or transmit data (NATO 2013). Some definitions highlight cyberspace through the visibility of physical or virtual interconnections (Ning et al. 2018), while others suggest it comprises multiple layers, including the physical, logical, and personal layers (Corn 2017). Additionally, it is viewed as an information-centred space, comprising a set of information objects, information systems, and websites within information and telecommunication networks, whose activities impact information formation and processing, from individual to public relations mechanisms (publication of legal acts unknown).

In summary, cyberspace is perceived as an immaterial and vast domain characterised by multi-layered connections in both physical and virtual realms. It spans from hardware to software and from raw data to structured information. Due to its complexity and openness, cyberspace remains highly vulnerable to attacks.

2.3 Navigate in the Intersection - The Offence-Defence Balance

The offence-defence balance theory has roots in the works of military theorists such as von Clausewitz (1976), who recognised that shifts in the balance of offensive and defensive capabilities could affect the frequency and duration of wars. It was traced back to conventional military and geographic domains, where defensive strategies leverage geographic advantages to better protect the territory, with larger territories offering benefits (Jervis 1978). At the same time, the offence shows the advantage when the technologies make the offensive postures and strategies less expensive (Lynn-Jones 1995). In this sense, Glaser & Kaufmann (1998) defined the office-defence balance as the ratio of costs the attacker requires to take down the territory and the defender's cost to deploy.

Technological advancements have made the failure of the offence-defence balance in cybersecurity a significant concern (Valeriano 2022). This imbalance arises when offensive capabilities outpace defensive measures, exacerbating vulnerabilities in cyberspace. As a result, tensions escalate, fostering an environment where actors can exploit the ambiguous boundaries of the grey zone.

Understanding and addressing this imbalance will ensure stability in cyberspace. It requires a multifaceted approach that combines technical, strategic, and policy-oriented perspectives to close the gap between offensive and defensive capabilities, thereby reducing opportunities for grey zone operations, which will be discussed in the following sections.

3. Methodology

It is hard to depict the overlap between the grey zone and cyberspace. The conceptual framework is a good start; Smyth (2004) defines it as the early stage tool as "a conception or model of what is out there that you plan to study." Luft et al. (2022) stated it as a method to "address gaps identified in the literature, clarify presumed relationships among concepts, and guide the overall direction of the study." Finally, Maxwell (2013) stresses that it is a product "not pre-existing entities; instead, they are constructed by researchers". These are composed of existing concepts but require an original structure and coherence that reflect the unique goals of the study. All of these support using the conceptual framework to develop the concept early.

In this research, the framework aligned with Gale et al. (2013) description as a set of codes organised into categories and collaboratively developed by researchers during the analytical process, allowing effective data management and organisation. The rationale for adopting this framework as the foundation lies in its dual capacity to function as both an entry-point structure for research and as an end product that is inherently interdisciplinary or multidisciplinary, as noted (Junghans & Olsson 2012).

The primary sources for constructing the framework include literature, theory, experience, and thought experiments (synthesis and speculative model-building) (Maxwell 2013, Ravitch & Riggan 2016, Smyth 2004). The literature and theoretical resources are limited, so the research emphasises experience and thought experiments more. Scholars such as Ravitch & Riggan (2016), Maxwell (2013), Marshall & Rossman (2014) and Robson and McCartan (2002) stress the importance of balancing personal insights with data from other sources achieved through observant practice and semi-structured interviews, which can be defined into two phases.

Phase 1: Established foundational insights through a systematic literature review on grey zone conflict, activities in cyberspace and the offence-deference balance, identifying recurring themes discussed in Section 2. These concepts were refined through observation practice at cybersecurity conferences, where practitioner discussions revealed real-world operational nuances. The observation practice involved attending seven relevant conferences. These conferences were differentiated based on the target audience, theme, or stated purpose. The Taiwan Academic Cybersecurity Center (TACC) is a national-level cybersecurity technology research centre highlighting a top-down national focus in cyberspace. On the other hand, the International Conference on Recent Advancements in Computing in AI, IoT and Computer Engineering Technology (CICET) has an academic research focus, bringing a bottom-up approach with its emphasis on technical aspects. International Conference on Cyber Conflict (CyCon) and European Conference on Cyber Warfare and Security (ECCWS) predominantly highlight the Western perspective with an international scope, featuring contributions from multiple countries. CyCon focuses on more government and military perspectives with minimal academic research involvement. In contrast, ECCWS emphasises academic research to influence governmental and military strategies. Responsible AI in the Military Domain Summit (REAIM) is also an international summit that focuses more on the military side with the government perspective; in 2024, it was hosted by Korea, injecting more of an Asia perspective into the discussion. Furthermore, the Hacks In Taiwan Conference (HITCON) has two conferences: one is focused on the community (CMT) with the students' clubs, and the other is more on the government and enterprise (ENT). These conferences revealed layers of focus, including technical aspects, strategic considerations, human resource engagement, data management, and legal framework, ranging from the individual focus to the international and stakeholders covering the academic, military, government and community.

Phase 2: Translate these insights into an initial framework structure, visualised as a framework to organise the interplay and thresholds in CGZ activities. The pyramid's layers were iteratively tested and refined using data from two in-depth case studies in the Taiwan Strait and NATO allies. The former faces severe cyberattacks and political pressure from China, which presents a particular case of the CGZ. In contrast, NATO-allied regions experience a markedly different set of challenges. Interviewees were carefully selected for their extensive experience and held managerial or high-level administrative roles. This ensured that the perspectives were from a holistic point of view, as required for the conceptual framework. The saturation data covered a wide range of expertise, from technology, strategy, operations, law, and education to the training to enhance the composition of the framework structure.

These data are analysed through Data analysis using Computer-Assisted Qualitative Data Analysis Software (CAQDAS), noted for its transparency and reliability in grounded theory research (Banner & Albarran 2009, Carcary 2011, Kapiszewski & Karcher 2021, O' Kane et al. 2021, Sinkovics & Alfoldi 2012). Grounded theory was

applied to conceptualise findings from research evidence rather than imposing pre-existing theories (Glaser et al. 2004), aligning with this study's focus on defining the CGZ.

In summary, with the research process mentioned in this section, the framework is expected to reach features identified as follows:

- An overarching schema to contextualise the CGZ, establishing relationships, fostering understanding, and encapsulating its defining characteristics and operational complexities.
- A dynamic CGZ model developed through rigorous data collection from semi-structured interviews, minimising bias, ensuring reliability, and integrating theories via grounded theory practices to reflect its nature.
- Supportive analytical data underpinning a narrative explanation of the CGZ, highlighting multi-domain interactions and visual representation across case studies.

4. Framework

4.1 Overview of the Structure

The framework's building blocks were systematically identified and validated through a three-stage process in the Phase 2. First, candidate blocks were derived from thematic patterns in the literature review (e.g., attribution challenges, escalation thresholds) and observations through participating conferences. For instance, discussions at CyCon and ECCWS repeatedly emphasised the interplay of legal ambiguity, political will, and technical feasibility in grey zone campaigns. These insights were formalised into distinct blocks such as "Legality and Political Will" and "Technical Analysis", ensuring the framework captured multidimensional drivers of CGZ activities.

Second, candidate blocks were iteratively tested against empirical data from case studies and through interviews. For example, the "Offence-Defence Balance" block—initially identified in the literature and echoed in CyCon debates on persistent engagement strategies—was refined to incorporate interview findings highlighting how states exploit deterrence gaps. Conversely, some proposed blocks were discarded during this stage. While literature and conferences frequently categorised actors as "state" or "non-state", interview data revealed that such distinctions did not meaningfully alter operational outcomes in practice. Consequently, "Actor" typologies were excluded from prioritising behavioural dynamics over institutional labels.

Finally, the remaining blocks were organised hierarchically into a pyramid structure to reflect interdependencies. The baseline for this composition was derived from the defining characteristics of the cyber grey zone: its position between legal and illegal operations, its activities below the threshold of armed conflict, and its dynamic nature shaped by offence, defence and threat intelligence operations; these characteristics informed the framework's foundational axis. The pyramid shape was chosen to represent this escalation visually. The pyramid's base corresponds to lower-tension activities, while the apex represents higher-tension actions closer to the threshold of kinetic warfare. The pyramid thus captures the progressive intensification and visualising how tensions escalate.

Building on this baseline, the blocks were organised hierarchically based on empirical insights from case studies and interviews. For instance, the placement of the Political Will block at the apex reflects a consensus from interviews: while technical and operational factors influence grey zone activities, the decision to escalate tensions towards kinetic warfare is ultimately driven by political considerations. This block's position underscores its role as the decisive factor in crossing the threshold from peacetime to conflict.

At the pyramid's foundation lies the Incident block, the starting point for all grey zone activities. Case studies revealed that while cyber incidents occur frequently worldwide, only a subset escalates to higher tension levels. From there, the framework progresses through strategic analysis and operational preparation blocks, reflecting the layered decision-making process observed in real-world scenarios.

4.2 Decomposition of Each Block

To align with the features outlined, the framework integrates insights summarised into five interconnected blocks - i) Incident, ii) Technical Analysis, iii) Strategic Context, iv) Operational Preparation, and v) Legality and Political Will. The x-axis represents a spectrum of activities ranging from legal to illegal, while the y-axis illustrates the role of threat intelligence connecting all blocks; all blocks apply to both offensive and defensive operations; case studies and broad references inform this structure. The framework, shown in Fig. 1, provides a general overview.

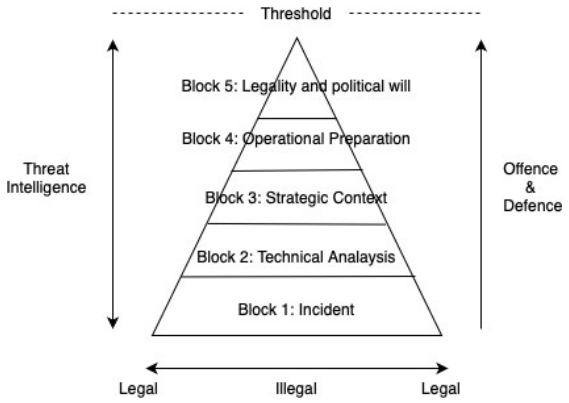

Figure 1: FCGZ Overview

4.2.1 Block 1: Incident

At the pyramid's base are specific cyber incidents, which serve as the starting point for analysis. These incidents are diverse and numerous. The case studies reveal that incidents are especially significant in shaping cyberspace dynamics and the broader grey zone landscape. These incidents fall into three categories - i) Disinformation, Defacement, and Distributed Denial-of-Service (DDoS) attacks, ii) Intelligence Gathering, iii) CI Disruption, representing varying complexity levels and potential consequences, forming the framework's foundation. Take the i) as an example:

i). Disinformation, Defacement, and Distributed Denial-of-Service (DDoS) attacks

Method: Spreading disinformation, compromising the integrity of publicly available internet-based services through defacement, and disrupting service availability. Purpose: To create societal instability by undermining public trust in authorities.

Purpose: To create societal instability by undermining public trust in authorities.

Note: These are disruptive but generally not destructive. Such actions might involve hacktivists or low-level cybercriminals, temporarily affecting systems without causing long-term damage.

4.2.2 Block 2: Technical analysis

Technical analysis in incident response follows a structured process: identifying potential issues, conducting investigations, reporting to senior leadership, and taking action. However, not all incidents are scrutinised due to the high volume of cyber activities. Leadership-driven investigations often receive more resources but may lack technical evidence, complicating efforts to trace issues to their origins. While triggering investigations, system alerts frequently produce false positives, leading to inefficiencies when defenders focus on metrics like alert counts instead of preventing future attacks. Hackers exploit this by using minimalistic, stealthy methods to evade detection. The emphasis on routine statistical reporting diverts attention from essential strategies like refining alert rules and performing correlation analysis, leaving root causes unaddressed.

Another limitation is technical analysts' lack of real-time authority, delaying containment and mitigation efforts. Streamlining decision-making and empowering experts to act promptly would significantly improve response efficiency. Reaction strategies must also be tailored to the specific context of each incident.

The primary goals of technical analysis are to attribute the source, understand the attackers' motivations, and conduct risk assessments, providing valuable insights for future defensive measures and decision-making.

4.2.3 Block 3: Strategic context

The third block examines the broader implications of incidents within the strategic landscape, particularly their alignment with geopolitical or organisational goals.

The case study demonstrates that each state has a fold of the strategy; take Taiwan as an example. Taiwan employs a three-level strategy to counter threats in CGZ, focusing on public awareness, defensive preparedness, and proactive resilience, which corresponds to the incident categories identified in Block 1, i.e. the Disinformation, Defacement, and Distributed Denial-of-Service (DDoS) attacks in the Block 1 is taking the

strategic action to react through the public awareness and stability program. These levels are designed to align with the escalating costs and impacts for both attackers and defenders. The mixed-strategy approach ensures flexibility in addressing varied threat levels. Take the Block 1 - Disinformation, Defacement, and Distributed Denial-of-Service (DDoS) attacks as an example; the strategy might correspond to – i) Conducting cyber awareness campaigns, ii) Strengthening real-time fact-checking mechanisms to prevent public panic and maintain societal stability.

It is not the one-to-one strategy that corresponds to the incident categories. Different states, organisations, and regions have different approaches. Still, it is applied as the mixed-strategy approach ensures adaptability, aligning defensive levels to counter escalating adversarial tactics.

4.2.4 Block 4: Operational preparation

There are various ways to address threats beyond the strategic context, with cyber operations being one component. This section focuses on the planning and readiness required for such operations, whether defensive or offensive. Activities in this phase often involve navigating complex legal and ethical boundaries.

Feedback from case studies highlights the importance of defining strategic intent before advancing to operational preparation. Once the potential consequences of an incident are understood, next is to plan an appropriate response, particularly when operations are conducted jointly with other states. Operational preparation often involves exercises and simulations that test and refine response strategies, enhance technical capabilities, and foster trust and collaboration among international partners.

Among these elements, trust—both between states and within states—emerges as a cornerstone. For example, Locked Shields, the largest multinational cyber exercise, highlights the importance of trust and cooperation across nations. Participating countries share knowledge and resources, fostering a unified defence approach. This exercise strengthens cross-national trust and encourages collaboration among cybersecurity professionals and policymakers.

4.2.5 Block 5: Legality and political will

Legality and political decision-making are at the apex of the pyramid, determining whether cyber incidents escalate into conflict or remain in cyberspace. While grey zone actions can cause disruptions, they rarely lead to war unless legal frameworks and political will align.

The legal ambiguity surrounding cyber activities makes escalation to warfare unlikely, as international law lacks clear definitions and thresholds for cyberattacks. Although most cyber actions do not lead to war, their impact can escalate, especially if targeting critical infrastructure or part of a coordinated strategy.

Cyber operations combined with political or economic influence require nuanced responses, as escalation thresholds are context-dependent. While cyber actions rarely cause physical harm, they can heighten tensions and potentially trigger larger conflicts. Extreme cases may prompt responses under international agreements like NATO's Article 5.

Ultimately, legality provides a framework for justifying actions. Still, politics ultimately determine escalation or containment, influenced by strategic priorities, domestic pressures, and global diplomacy, to decide whether to cross the threshold into kinetic warfare.

5. Reflection and Discussion

The proposed framework for conceptualising CGZ activities offers a structured, multi-method approach synthesising qualitative insights with theoretical grounding. While its ambition to systematise the CGZ is commendable, several methodological and conceptual limitations warrant deeper scrutiny, raising questions about its theoretical rigour, representational accuracy, and practical utility.

5.1 Methodological Concerns: Subjectivity and Epistemological Rigour

The framework's reliance on qualitative data —case studies, interviews, conference observation and materials —introduces epistemological vulnerabilities. The selection of literature and case studies risks inherent bias, as the source inclusion/exclusion criteria are time and region-justified. For instance, academic and conference sources were prioritised based on geographic dichotomies: only Taiwan and Western-centric perspectives. The decision to discard actor typologies based on interview feedback exemplifies this issue. While pragmatic, it sidesteps the nuanced motivations of state versus non-state actors, potentially flattening critical distinctions in

CGZ dynamics. This raises concerns about whether the framework's development validated pre-existing assumptions.

5.2 Structural Flaws: The Illusion of Linearity

Though visually intuitive, the pyramid structure imposes a reductive linearity on CGZ phenomena. The framework neglects cyber conflict's non-linear and recursive nature by framing escalation as a hierarchical progression from technical incidents to political decisions. In reality, de-escalation, parallel campaigns, and feedback loops (e.g., technical vulnerabilities exposed by strategic actions) are endemic to cyber operations. The pyramid's apex—political will—is presented as a discrete driver, yet political and technical layers are often entangled; for example, political agendas may directly shape the tools available to operatives. This compartmentalisation risks misrepresenting how systemic interactions drive CGZ activities, privileging simplicity over accuracy.

5.3 Generalisability and Temporal Blind Spots

The framework's empirical foundations are narrowly constructed. Its cases and conference sources likely reflect specific geopolitical contexts in parts of Europe and Taiwan, limiting applicability to regions with differing norms. Moreover, the rapid evolution of cyber threats—such as AI-driven attacks or ransomware ecosystems—is not addressed. The framework risks obsolescence upon publication if case studies are drawn from outdated examples. Broader validation across diverse contexts and emerging trends is essential to ensure relevance.

6. Conclusion

The challenge of addressing CGZ activities lies in their inherent ambiguity: they exploit conflict thresholds, operate in legal and political liminality, and blur distinctions between peacetime and warfare. This research confronts these complexities by proposing a structured framework—organised into five analytical blocks—to dissect CGZ phenomena systematically. By breaking down cyber operations into discrete yet interconnected dimensions, the framework offers a pragmatic tool for policymakers and analysts to navigate the opacity of CGZ tactics, assess their escalation risks, and devise context-specific responses.

The framework's strength lies in its ability to generalise insights without oversimplifying context. Categorising incidents into blocks enables triaging threats, identifying leverage points, and evaluating proximity to conflict thresholds. However, the analysis also reveals limitations: the pyramid's linearity risks oversimplifying feedback loops, and the exclusion of actor typologies obscures divergent motivations between state and non-state actors.

To strengthen the framework's applicability, future research could prioritise testing the framework against diverse geopolitical contexts to identify region-specific norms and escalation triggers, Incorporate emerging trends such as AI-driven disinformation, replacing the static pyramid with adaptive models, and develop scenario-based training modules to help policymakers apply the framework in crisis simulations, ensuring it informs real-time decision-making under uncertainty.

The evolving nature of cyber threats demands agility: static models risk obsolescence as adversaries innovate. By addressing its structural limitations and expanding its empirical scope, this framework could evolve into a living tool that interprets the grey zone and anticipates its next contours. In a domain defined by flux, resilience lies not in rigid taxonomies but in adaptive, interdisciplinary thinking.

References

Bajec, A. (2023) 'The growing diplomatic backlash against Israel's war on Gaza', The New Arab. Available at: https://www.newarab.com/analysis/growing-diplomatic-backlash-against-israels-war-gaza (Accessed: 26 June 2024).

Banner, D. and Albarran, J. (2009) 'Computer-assisted qualitative data analysis software: A review', Canadian Journal of Cardiovascular Nursing, 19(3).

Carcary, M. (2011) 'Evidence analysis using CAQDAS: Insights from a qualitative researcher', Electronic Journal of Business Research Methods, 9(1), pp. 10–24.

Command, U.S.S.O. (2015) 'The grey zone', White Paper.

Corn, G. (2017) 'Cyber national security: Navigating grey zone challenges in and through cyberspace', Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare (2018, Forthcoming).

Dobbs, T., Fallon, G., Fouhy, S., Marsh, T. and Melville, M. (2020) 'Grey-zone activities and the ADF: A Perry Group report'.

Gale, N.K., Heath, G., Cameron, E., Rashid, S. and Redwood, S. (2013) 'Using the framework method for the analysis of qualitative data in multi-disciplinary health research', BMC Medical Research Methodology, 13, pp. 1–8.

Glaser, B.G., Holton, J. et al. (2004) 'Remodelling grounded theory', Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, 5.

Glaser, C.L. and Kaufmann, C. (1998) 'What is the offense-defense balance and can we measure it?', International Security, 22(4), pp. 44–82.
Hoffman, F.G. (2007) Conflict in the 21st century: The rise of hybrid wars, Potomac Institute for Policy Studies, Arlington.
Jervis, R. (1978) 'Cooperation under the security dilemma', World Politics, 30(2), pp. 167–214.
Jordan, J. (2020) 'International competition below the threshold of war', Journal of Strategic Security, 14(1), pp. 1–24.
Joyce, S. and Huntley, S. (2024) 'Tool of first resort: Israel-Hamas war in cyber', Google Blog. Available at: https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber/ (Accessed: 26 June 2024).
Junghans, A. and Olsson, N. (2012) 'Does facilities management meet the requirements of an academic discipline?', Proceedings of the Joint CIB W70.
Kapiszewski, D. and Karcher, S. (2021) 'Transparency in practice in qualitative research', PS: Political Science & Politics, 54(2), pp. 285–291.
Kiessling, E.K. (2021) 'Gray zone tactics and the principle of non-intervention: Can one of the vaguest branches of international law solve the gray zone problem?', Harvard National Security Journal, 12, pp. 116–137.
Krishnan, A. (2009) 'What are academic disciplines?', Some Observations on the Disciplinarity vs. Interdisciplinarity Debate, pp. 1–59.
Layton, P. (2022) 'China's grey-zone activities: Concepts and possible responses', Journal of the Royal New Zealand Air Force, 7(1-2022).
Liang, Q. and Xiangsui, W. (1999) Unrestricted warfare, Citeseer.
Luft, J.A., Jeong, S., Idsardi, R. and Gardner, G. (2022) 'Literature reviews, theoretical frameworks, and conceptual frameworks: An introduction for new biology education researchers', CBE—Life Sciences Education, 21(3), rm33.
Lynn-Jones, S.M. (1995) 'Offense-defense theory and its critics', Security Studies, 4(4), pp. 660–691.
Maass, R.W. (2022) 'Salami tactics: Faits accomplis and international expansion in the shadow of major war (Winter 2021/2022)', Texas National Security Review.
Marshall, C. and Rossman, G.B. (2014) Designing qualitative research, Sage Publications.
Maxwell, J.A. (2013) Qualitative research design: An interactive approach, Sage Publications.
NATO (2010) 'Strategic concept 2010'. Available at: https://www.nato.int/cps/en/natohq/topics_82705.htm (Accessed: 20 December 2024).
NATO (2013) 'Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations'. Available at: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations (Accessed: 21 August 2024).
Ning, H., Ye, X., Bouras, M.A., Wei, D. and Daneshmand, M. (2018) 'General cyberspace: Cyberspace and cyber-enabled spaces', IEEE Internet of Things Journal, 5(3), pp. 1843–1856.
O'Rourke, R. (2020) US-China strategic competition in South and East China Seas: Background and issues for Congress, Congressional Research Service, Washington, DC.
O'Kane, P., Smith, A. and Lerman, M.P. (2021) 'Building transparency and trustworthiness in inductive research through computer-aided qualitative data analysis software', Organizational Research Methods, 24(1), pp. 104–139.
Publication of Legal Acts (unknown) 'Presidential decree of 12.5.2016 number 646: On approval of the doctrine of the Russian Federation information security'. Available at: http://publication.pravo.gov.ru/Document/GetFile/0001201612060002?type=pdf (Accessed: 25 May 2024).
Ravitch, S.M. and Riggan, M. (2016) Reason & rigor: How conceptual frameworks guide research, Sage Publications.
Robson, C. and McCartan, K (2002*) Real world research*. 2nd edn. Oxford: Blackwell.
Ryan Shandler, D.C. and Mimran, T. (2024) 'A look inside the cyberwar between Israel and Hamas reveals the civilian toll', The Conversation. Available at: https://theconversation.com/a-look-inside-the-cyberwar-between-israel-and-hamas-reveals-the-civilian-toll-228847 (Accessed: 26 June 2024).
Sari, A. et al. (2024) Hybrid threats and grey zone conflict: The challenge to liberal democracies, Oxford University Press.
Service, E.E.A. (2018) 'A Europe that protects: Countering hybrid threats'. Available at: https://www.eeas.europa.eu/node/46393_en (Accessed: 20 December 2024).
Sinkovics, R.R. and Alfoldi, E.A. (2012) 'Progressive focusing and trustworthiness in qualitative research: The enabling role of computer-assisted qualitative data analysis software (CAQDAS)', Management International Review, 52, pp. 817–845.
Smyth, R. (2004) 'Exploring the usefulness of a conceptual framework as a research tool: A researcher's reflections', Issues in Educational Research, 14(2), pp. 167–180.
Strachan, H. (2021) 'Global Britain in a competitive age: Strategy of the integrated review', Journal of the British Academy.
Update, D.S. (2020) 'Electronic resource', Australian Department of Defence. Available at: https://www.defence.gov.au/about/publications/2020-defence-strategic-update (Accessed: 23 July 2023).
Unit42 (2024) Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns. Available at: https://unit42.paloaltonetworks.com/i-soon-data-leaks/ (Accessed 4 March 2025).
Valeriano, B. (2022) 'The failure of offense/defense balance in cyber security', The Cyber Defense Review, 7(3), pp. 91–102.
von Clausewitz, C. (1976) On war, Princeton University Press, Princeton, NJ.