Exploring Cyberspace and the Grey Zone: Insights from Multistakeholder Perspectives

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: Cyber operations link the virtual and physical worlds, involving diverse stakeholders, including civilians, governments, academics, and the military. This research addresses gaps in understanding cyberspace and the grey zone, which is conventionally seen as the area between peacetime and wartime with legal to illegal behaviour, and implications on attack and defence strategies through insights gained from conferences and workshops. An observational study of the various stakeholder communities was undertaken from seven events spanning academia, government. Community perspectives were surfaced using onsite observation, note taking for the presentation sessions and keynotes, with the Computer-Assisted Qualitative Data Analysis Software (CAQDAS) used to conduct data analysis and to develop new insights. The themes identified include current dynamics (The horizon), preparation (On the horizon), next steps (Over the horizon), and audience interactions (In the room). These observations provide a nuanced understanding of contemporary cyber conflict and strategic approaches to cybersecurity.

Keywords: Cyber grey zone, Grey zone, Cyberspace, Cyber conflict, Cyber operations

1. Introduction

As new technologies evolve, the grey zone and activities in cyberspace are becoming focal points of academic and practical discourse. Despite their growing importance, limited literature examines these perspectives across diverse stakeholders, including academia, government, industry, the military, and various levels, from individuals to international organisations.

Conferences, workshops, and seminars provide valuable venues for these stakeholders to exchange view, offering insights that traditional research publications often cannot capture. To explore these perspectives systematically, this research employs observational practices grounded in qualitative methodologies, supported by Computer-Assisted Qualitative Data Analysis Software (CAQDAS). This approach enables a structured and rigorous analysis to address the critical research question: how do stakeholders interpret and implement the concepts of cyberspace and the grey zone in their respective domains?

2. Literature Review

2.1 What's the Grey Zone

Liang & Xiangsui (1999) introduced the concept of *Unrestricted Warfare*, outlining a strategy that leveraged non-military means, such as economic and cyber warfare, to achieve strategic objectives without engaging in traditional military conflict. This marked the inception of what is now recognised as the grey zone.

Hoffman (2007) expanded the concept, describing it as combining conventional and unconventional tactics that remain below the threshold of full-scale warfare but exceed regular interstate competitive interactions. Brands (2016) defined grey zone conflict as coercive and aggressive activities intentionally kept below the threshold of open warfare to minimise risks and penalties associated with direct conflict. Similarly, Green et al. (2017) characterised it as efforts to achieve security objectives by operating beyond stable deterrence without resorting to large-scale military force, carefully avoiding actions that might escalate to war. Jordan (2020) described the grey zone as the intermediary space between peaceful relations and armed conflict, where strategic competition occurs below the threshold of war. It is a space separating conventional political competition from outright armed confrontation within the spectrum of political conflict.

The summarised characteristics of the grey zone, as drawn from Hoffman (2007), Brands (2016), Tovo et al. (2016), Green et al. (2017), Jordan (2020), O'Rourke (2020), Dobbs et al. (2020), Layton (2022), Strachan (2021), Kiessling (2021), Maass (2022), and Sari et al. (2024) are presented below:

- **State and non-state actors** Involvement.
- Lies between the concepts of **traditional warfare and peace, below the threshold of the armed conflict**

- Ambiguity and uncertainty with **military and non-military** means are critical characteristics, making it a complex, challenging and coercive environment.
- The **conventional and unconventional techniques** have significant implications for national security interests, requiring careful consideration and analysis.
- Between **legality and illegality** in international norms and difficulties of attribution.
- The effect is **incremental escalated**, or described as the "Salami-slicing", "creeping norms", or "faits accomplis". Actors gradually increase pressure to test response thresholds and beat others through "losing without fighting" to avoid triggering a strong response

2.2 Cyberspace

The definition of cyberspace has been debated since 1982, when William Gibson, a science fiction author, first coined the term. The discussion has persisted for decades without a definitive conclusion, as cyberspace embodies both abstract and tangible elements, engaging academics, practitioners, and governments alike. This complexity has hindered the development of a precise, scientific definition, as noted by Garvey (2021).

Starodubtsev et al. (2020) underscore the diverse interpretations of cyberspace despite extensive research dedicated to the subject. They argue that the need for a unified definition complicates theoretical and practical advancements in politics, economics, and societal contexts. Their review highlights how the absence of a consistent framework impedes the efficient application of cyberspace in these domains.

Scholars have approached cyberspace from varied perspectives. Ning et al. (2018) propose the concept of reshaped general cyberspace, which integrates physical, social, and cognitive spaces through ubiquitous connectivity. This view extends beyond traditional distinctions between physical and virtual realms, encompassing the interplay of cyber elements within human cognition and activity. Within the Cyber Conceptual Framework, Ormrod et al. (2016) define cyberspace as comprising physical and virtual domains nested within national security frameworks. Their model highlights its pivotal role across political, economic, and military spheres, reflecting cyberspace's multi-faceted and evolving significance.

Cyberspace is inherently multifaceted, transcending logical and physical boundaries to encompass psychological and cognitive aspects with multi-disciplinary implications.

3. Methodology

3.1 Qualitative Data Analysis

The foundational methodology used in this study is grounded theory, as elucidated by Glaser et al. (1967). Traditionally associated with qualitative research, grounded theory involves deriving theory from empirically gathered data and is chosen for this research because it focuses on conceptualising from research evidence rather than imposing theories (Glaser et al., 2004).

Computer-Assisted Qualitative Data Analysis Software (CAQDAS) is widely used to conduct qualitative data analysis (Banner and Albarran, 2009). The methodological foundations of CAQDAS have been studied and recommended for application in grounded theory (Carcary, 2011; Sinkovics et al., 2012) due to their ability to enhance transparency and reliability in the data analysis process (Kapiszewski et al., 2021; O'Kane et al., 2021). QualCoder is applied to this study among CAQDAS tools for conducting data coding, a fundamental component of the systematic analytical process in qualitative research. This data coding enables the deconstruction of data into raw empirical elements, facilitating new insights and more profound understanding (Elliott, 2018). Initially, descriptive coding was performed at the surface level to highlight relevant data (Saldana, 2021). However, the initial coding process produced an excess of labels. Similar labels were merged into unified coding schemes to ensure qualitative analysis consistency, as Zhang (2009) recommended. This practice involved importing conference notes into a database and conducting descriptive coding by highlighting keywords or phrases and categorising them (e.g., "manpower"). Subsequently, similarly labeled categories were compared and analysed to uncover insights, such as identifying "cooperation" and "trust" as key factors in "manpower" and exploring their significance across different conference perspectives. The evolution of the coding labels was dynamic, involving numerous revisions before arriving at the final version.

3.2 Benefit of Attending Conferences

Hickson (2006) emphasises that professional conferences keep researchers engaged and active in their fields. These events provide opportunities to collaborate, network, and explore new developments. They also serve as

platforms for connecting researchers, vendors, and policymakers to exchange expertise and perspectives (McCurry, 2024).

The sensitive and secretive nature of cyberspace and grey zone issues, often tied to national interests, can make participant observation challenging. For instance, González's (2012) experience with the US Pentagon programme underscores the difficulties in accessing military organisations and classified topics. Nader's (1972) recommendation of adopting diverse perspectives—``up, down, and sideways''—is applied to address these barriers. In this study, seven conferences have been selected for observational practice. These span international, national, and individual focuses and cover perspectives from academia, the military, government, and the community.

3.3 Conference Selection Justification

Seven conferences were selected for their relevance to cyber conflict and cybersecurity, spanning technical, operational, and strategic domains and individual, national, and international perspectives. 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 the 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 venues: one is focused on the community (CMT) with the students' clubs, and the other is more on the government and enterprise (ENT).

The primary observations were centred on the intersection between cyberspace and the grey zone and have been categorised into four areas:

1. The Horizon (Section 4.1): This section represents the current overlap status between cyberspace and the grey zone. It includes the speaker's views on the dynamics within this area.
2. On The Horizon (Section 4.2): This section reflects the state of preparation and readiness derived from the feedback received during the conference.
3. Over The Horizon (Section 4.3): This section discusses how emerging technologies change the intersection dynamics between cyberspace and the grey zone.
4. Lastly, In The room (Section 4.4) provides an overview of the overall physical atmosphere of the environment and the attitudes observed among the audience. This section comprehensively explains the audience's reactions and interactions during the events.

Each area provides perspective on the interplay between cyberspace and the grey zone, generated and concluded by speakers in the conference offering insights into the current state of affairs and future trends.

4. Themes

4.1 The Horizon - Status

The boundaries between cyberspace and the grey zone are ambiguous, as covered in the Literature Review. Whether cyberspace encompasses the grey zone or overlaps remains undefined. However, there is a consensus on an area representing strategic competition below the threshold of armed conflict (CyCon).

Below the threshold of armed conflict has been mentioned many times throughout the CyCon. Still, without a precise definition, the likely definition is provided in the ECCWS, which presents a study exploring operations above and below the threshold, examining various cyber-capabilities. It proposes a multi-level, multi-aspect architecture that encapsulates conflict dynamics, utilises multiple instruments of national power, and engages alliances across physical, virtual, and psychological domains. The study identifies the threshold of armed conflicts at Level 3 (offensive cyber-physical) and Level 2 (cyber and information boundary). Levels 0 and 1 involve intelligence collection and influence campaigns, while Levels 4 and 5 correspond to kinetic conventional military campaigns and nuclear warfare, respectively (ECCWS).

In the context of power that leads to crossing the threshold of armed conflicts, actors are categorised into internal and external entities or state and non-state actors. External entities encompass a variety of actors, including nation-states, hackers, terrorist groups, and criminal organisations.

On the other hand, internal threats comprise insider threats, rogue employees, domestic extremist groups, media companies, and even unsuspecting customers. From the other perspective, the distinction between state and non-state actors is intuitive, based on whether a state is involved in the activity. State actors are particularly noteworthy due to the significant resources and capabilities supported by states to execute sophisticated attacks with political, economic, or military objectives. Non-state actors are driven by ideological goals or financial gain (CyCon, ECCWS).

Although actor categories are proposed, attribution challenges include misattribution, understanding technique-tactic procedures, linguistic analysis, and attribution in the digital fog (ECCWS). Various techniques such as malware analysis, network traffic analysis, digital forensics, AI, and machine learning address these challenges (ECCWS, TACC, CiCET). However, ethical, legal, and political considerations can complicate these efforts (CyCon).

Even though there is a challenge of the attribution, there is consensus regarding state actors who post threats through the offensive operation; Russia is explicitly mentioned in CyCon and ECCWS, China is mentioned in CyCon, TACC, CiCET, and North Korea is mentioned in ECCWS.

Offensive operations in cyberspace exploit vulnerabilities to disrupt adversaries' operations. Their success hinges on three criteria: clear objectives, access requirements, and the correct payload (for the malware's technical binary and the influence operation's informational content), which have policy, technical, and legal implications (ECCWS). Take the Ukraine-Russia case as an example; DDoS attacks, malware, ransomware, and wiper attacks aim to disrupt services, interfere with elections, damage critical infrastructure, and compromise data and communication are counted for the offensive operations; information operations are part of the toolkit (ECCWS).

4.2 On the Horizon - Preparation

Considering the asymmetrical nature of the threat (CyCon), a defence strategy with multiple layers incorporating preventive and responsive actions is essential (ECCWS).

NATO, Indo-Pacific Pacific, and the US strategic perspectives were presented in the CyCon. From the Indo-Pacific Perspective, the restructuring of cyber power in China and Russia is observed. NATO's situations emphasise resilience and proactive engagement to shape this adversary's behaviour by prioritising integrating military capabilities. This engagement is further elucidated by the US approach to cyber operations and the concept of persistent engagement, competition, and international collaboration. It is noted that cyberspace is a continuously contested environment, with routine cyber operations below the threshold of armed conflict. A proactive campaigning approach is advocated to disrupt and contest adversary behaviour, all while avoiding escalation to armed conflict (CyCon).

As the evolving contemporary conflicts, traditional principles may only partially align with current state practices. Collective countermeasures as the whole-of-nation, even the whole-of-international, are suggested to serve as a middle ground to avoid escalation to self-defence while still addressing wrongful acts, even under concerns about the reluctance of states to publicly declare their positions on countermeasures due to risks like attribution and operational security (CyCon, ECCWS, TACC, CiCET) as below:

- About manpower - Cooperation and Trust

The landscape faces a critical challenge in attracting and retaining talented individuals, particularly within the academic and military sectors (TACC, CyCon, ECCWS). Although these sectors struggle with recruitment, retention, and promotion, the broader perspective reveals that all contributions, regardless of where these individuals work, serve a unified national interest. In this sense, the focus shifts from individual sectors to a comprehensive, whole-of-nation approach, where the efforts of all professionals contribute to a collective goal of national security (CyCon, TACC).

Cross-domain cooperation underpins the national strategy, integrating efforts across academia, industry, government, and the military to enhance multi-domain operations. Trust is critical, fostering civilian-military collaboration, public-private partnerships, and international cooperation (CyCon, ECCWS). Building on this foundation, proactive measures, agility, and synergy in cross-domain responses are developed.

- About Data power - Information and Intelligence

The success of threat intelligence relies on data-driven strategies. ECCWS outlines eight principles to overcome barriers in policy, processes, and personnel, while CyCon discusses intelligence principles at international and national levels. Both highlight the value of private-sector expertise and the challenges of communication and integration across sectors.

ECCWS emphasises streamlined policies, interoperability, joint tool development, reducing bureaucracy, fostering shared risk-benefit cultures, incentives, and strong leadership. CyCon explores the evolution of cyber intelligence, regional tensions, OSINT's role, and the need for resilience, data-driven operations, and intelligence sharing based on recent conflicts.

CiCET and CyCon note the importance of collaboration within NATO but acknowledge the need for different approaches for non-aligned contexts, contrasting ECCWS's detailed framework for building alliances. Both stress cyber intelligence's rapid evolution and integration into national defence, focusing on holistic strategies, resilience, and readiness against sophisticated threats.

- About Legal power

A robust legal framework in cybersecurity is essential to prevent undesirable consequences and ensure clarity in legal theory and practice (ECCWS). However, the current framework faces significant challenges on both the offence and defence sides, leading to misinterpretation and hindering the development of international norms (CyCon).

In CyCon, the legal discourse among states grapples with the challenge of advocating for collective countermeasures while exercising caution. Considering potential legal implications and historical precedents, this approach is particularly relevant to the military. It is highlighted that the limits and scope of these measures should be defined to prevent misuse and to avoid undermining the role of the UN Charter and the Security Council. The objective is to ensure that collective countermeasures supplement rather than supplant. In contrast, the ECCWS focuses on discussing cyber fraud in general, which is more pertinent to civilians' daily lives. However, these discussions have common threads, such as the attribution of actors, case identification, interpretation of lawfulness, and reporting and response mechanisms.

Moreover, the legal framework is still evolving, and the focus must be on refining principles and guidelines to bolster global governance without escalating conflicts. Future strategies should focus on enhancing corporate governance around security, integrating security by design, combating misinformation, and deploying AI responsibly. Transparency, accountability, and continuous improvement are fundamental to successfully implementing defence measures and ethical practices and addressing overlooked issues in cybersecurity.

Improving the legal framework necessitates a balance in the scope of analysis, identification of common understandings among state positions, and addressing methodological issues in the development of international law. Internal discussions within government can enhance consistency in policy and legal interpretations. Future directions should explore how national positions can address emerging legal questions and integrate insights from various fields to inform international law development effectively.

4.3 Over the Horizon - AI and Quantum

The influence of emerging technologies, particularly Artificial Intelligence (AI) and quantum techniques, has become increasingly significant. These technologies are transforming military capabilities by enabling the development of advanced cyber capabilities, autonomous platforms, and sophisticated cryptographic tools. Discussions at ECCWS, CyCon, and TACC have highlighted the profound impact of these technologies on cybersecurity, specifically regarding their implications for government and military strategies. From a technical perspective, CiCET has emphasised the potential influence of these technologies on cyberspace. Meanwhile, REAIM has underscored the role of AI in driving conflict in cyberspace and even cyber warfare.

Post-quantum cryptography (PQC), which involves cryptographic algorithms resistant to attacks from quantum computers, is being developed and standardised to safeguard digital communications against future threats posed by quantum computing. This development underscores the importance of preparing for a future where quantum capabilities could compromise security measures (CyCon, TACC).

Conversely, AI introduces risks such as lack of explainability, automation bias, and potentially lowering ethical standards in warfare. These concerns emphasise the need for careful governance, ethical deployment, and continuous refinement of AI systems to mitigate risks and ensure they enhance rather than undermine security.

The complexity of AI systems also presents challenges in military contexts, where explainability and compliance with international humanitarian law are crucial (ECCWS, CiCET, CyCon).

Both AI and quantum technologies are reshaping the cyber landscape, necessitating new approaches to governance, security design, and not only a legal but also a good framework to manage their impact and ensure they are utilised responsibly to envision the future governance for AI in the military (REAIM).

4.4 In the Room – The Physical Atmosphere

These conferences present unique perspectives, and the distinct atmosphere is striking.

At CiCET and HITCON (CMT), participants adopt a more casual approach, while attendees at TACC and HITCON (ENT) lean towards business casual attire. CyCon, on the other hand, has a more formal atmosphere, with some military officers donning their uniforms, complete with ranks and medals. Others opt for business attire, as suggested on the conference's practical information webpage. At REAIM, many high-level government and military officers attend the ministerial roundtable session. This session features a diverse group of representatives from countries such as Malaysia, Singapore, Spain, Kenya, Canada, Ghana, Uzbekistan, Cameroon, Russia, and even China. Representatives with military, foreign affairs, and digital affairs backgrounds come together to discuss national approaches, priorities, and best practices on responsible AI in the military domain, addressing concerns and challenges and exchanging converging and diverging views and prospects for international cooperation.

CiCET and TACC are welcoming environments where unregistered individuals can sit and listen. In contrast, CyCon requires paid tickets, with security personnel at the main entry checking for badges. During the workshop day, strict registration for each session is mandatory.

Geographically speaking, the conference counts for more geographical advantage. In other words, the conferences hosted in the western part have more regional attendance. For example, CiCET and TACC consist entirely of Asian participants, while ECCWS has more Western attendees. Strategy-level conferences like CyCon and REAIM have a more mixed attendance.

Regarding the expertise focus, CyCon was assumed to be a strategy-level conference. Still, in 2024, through conversational observation, it was noted that two participants who played the HITCON Capture The Flag (CTF) game, which is typically a technical competition for offensive and defensive cybersecurity, were present. TACC is a melting pot of presenters who were once technical experts but now hold more managerial or directional positions. CiCET, with its narrow technical focus, almost none had policy or strategy-level backgrounds. ECCWS break rooms cover a wide range, from educational strategy and technical details of sensors and detection to management-level frameworks and new technologies like AI.

HITCON is a unique conference that brings the community tightly together. Throughout the year, the organisation hosts events catering to different needs, and participants attend not only one but multiple events, targeting different areas. In July, HITCON (CMT) is regularly used for technical purposes, and the HITCON CTF is shared in September. In October, the HITCON CISO Summit targets high-level managers in the industry and government sectors. HITCON (ENT) further brings the management and strategy levels together, aligning industry and government needs.

5. Reflection and Discussion

5.1 The gap Between Technical Focus and Strategy Focus

There are evident gaps between the technical, management, and strategic levels in conference publications and discussions. For instance, CiCET focuses on machine learning and AI, and TACC emphasises cybersecurity despite its national strategy support and efforts to facilitate cross-ministry collaboration. CyCon adopts a government and military perspective, where participants discuss high-level interests and strategies at the international level; ECCWS, on the other hand, covers a broad range of topics primarily related to defence development. Further details are provided below: The CiCET and TACC conferences concentrate solely on artificial intelligence and cybersecurity, emphasising technical research's specialised and isolated nature. In contrast, although CyCon and ECCWS encompass a broad range of topics, from technical to non-technical, these subjects are addressed independently, and there is no shared platform for comprehensive discussion. This separation contributes to misunderstandings, as researchers may concentrate on incremental advancements without considering broader implications, and strategists may overlook technical constraints. The absence of integrated dialogue at conferences such as CyCon and ECCWS inhibits the exchange of ideas between different disciplines.

Consequently, high-level strategies may be ineffective if technical limitations are not considered, potentially resulting in security vulnerabilities and missed opportunities for innovation. Furthermore, policymakers may fail to establish supportive frameworks for technological progress.

5.2 Cooperation is Everywhere and at Every Level

CiCET focuses on technical collaboration in cybersecurity and information technology, with a regional emphasis in Asia, particularly Taiwan, to foster academic cooperation by addressing technical challenges.

REAIM, co-hosted by Korea and nations like the Netherlands, Singapore, Kenya, and the UK, highlights evolving military cooperation beyond traditional alliances. Korea's role demonstrates its growing influence in defence-related AI technologies, contributing to global discussions on the ethical use of AI in warfare. REAIM brings together global stakeholders and breaks the traditional geographic barrier to embrace African, European, American, and Asia governments and militaries to develop responsible AI defence frameworks, ensuring AI's ethical deployment in military contexts. CyCon emphasises the need for strategic cooperation between governments to secure national and international cybersecurity. Addressing cyber defence, infrastructure protection, and digital sovereignty, CyCon helps shape international law and military strategies, fostering collaboration to address shared challenges in cyberspace.

TACC bridges national strategy with technological development. Directing funding towards cybersecurity priorities promotes collaboration among the private sector, academia, and government. This approach aligns research with national defence strategies, creating a cybersecurity ecosystem that drives innovation and shapes broader national security policies.

5.3 Effort from the Community

Among the various conferences, HITCON has been identified as hosting two annual events, each catering to distinct target audiences: one directed at students and community members primarily from the CMT sector and the other at enterprises, chiefly from the ENT sector. In addition to these conferences, HITCON has also organised other initiatives to strengthen the cybersecurity ecosystem in Taiwan. These efforts include training sessions led by experts who offer hands-on workshops in web security, mobile security, Linux systems, reverse engineering, forensics, and operational technology security. Furthermore, HITCON has facilitated the Free Talk and the Chief Information Security Officer (CISO) Summit. The former, a free forum established in 2014, encourages in-depth technical discussions on recent, high-profile cybersecurity incidents, while the latter invites representatives from Taiwan's top 100 publicly listed companies, leading cybersecurity enterprises, and governmental bodies in the Asia-Pacific region. The organization is recognised as a grassroots initiative in Taiwan, tirelessly working to continuously empower the cybersecurity community with innovation and resilience, contributing to improving Taiwan's cybersecurity ecosystem through fostering collaboration, innovation, and education.

6. Conclusion

Cyberspace and the grey zone are drawing attention from all levels worldwide. Through the conference attendance, the implication of multi-stakeholder insights is explored. Although conferences are hosted for different purposes, the combined efforts of academics, governments, military bodies, and grassroots communities demonstrate a shared commitment to addressing the complexities of cybersecurity and the grey zone. These stakeholders work tirelessly to adapt to emerging threats and foster innovation, ensuring that cybersecurity frameworks remain robust. As the landscape evolves, resilience will be paramount, requiring sustained cooperation, adaptability, and the proactive engagement of all parties to secure a safer digital future.

References

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

Brands, H. (2016). Paradoxes of the gray zone. Available at SSRN: https://ssrn.com/abstract=2737593.

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

Dobbs, T., Fallon, G., Fouhy, S., Marsh, T. & Melville, M. (2020). Grey-zone activities and the ADF: A Perry Group report.

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. *Qualitative Report*, 23(11).

Garvey, M.D. (2021). A philosophical examination on the definition of cyberspace. In Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions. *World Scientific*, pp. 1–11.

Glaser, B.G. & Strauss, A. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine Transaction.

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

González, R.J. (2012). Anthropology and the covert: Methodological notes on researching military and intelligence programmes. *Anthropology Today*, 28(2), pp. 21–25.

Green, M., Hicks, K., Cooper, Z., Schaus, J. & Douglas, J. (2017). Countering coercion in maritime Asia: The theory and practice of gray zone deterrence. *Rowman & Littlefield*.

Hickson, I.M. (2006). Raising the question: Why bother attending conferences? *Communication Education*, 55(4), pp. 464–468.

Hoffman, F.G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies, Arlington.

Jordan, J. (2020). International competition below the threshold of war. *Journal of Strategic Security*, 14(1), pp. 1–24.

Kapiszewski, D. & 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.

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. & Xiangsui, W. (1999). Unrestricted Warfare. Citeseer.

Maass, R.W. (2022). Salami tactics: Faits accomplis and international expansion in the shadow of major war. *Texas National Security Review*.

Nader, L. (1972). Up the anthropologist: Perspectives gained from studying up. ERIC.

Ning, H., Ye, X., Bouras, M.A., Wei, D. & Daneshmand, M. (2018). General cyberspace: Cyberspace and cyber-enabled spaces. *IEEE Internet of Things Journal*, 5(3), pp. 1843–1856.

Ormrod, D. & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence Studies*, 16(3), pp. 270–298.

O'Kane, P., Smith, A. & 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.

O'Rourke, R. (2020). US-China strategic competition in South and East China Seas: Background and issues for Congress. Congressional Research Service, Washington, DC.

Saldaña, J. (2021). The coding manual for qualitative researchers. SAGE Publications Ltd.

Sari, A. et al. (2024). Hybrid threats and grey zone conflict: The challenge to liberal democracies. *Oxford University Press.*

Sinkovics, R.R. & 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.

Starodubtsev, Y.I., Balenko, E., Vershennik, E. & Fedorov, V. (2020). Cyberspace: Terminology, properties, problems of operation. *In 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). IEEE*, pp. 1–3.

Strachan, H. (2021). Global Britain in a competitive age: Strategy of the integrated review. *Journal of the British Academy*.

Tovo, K., Spitaletta, J., Rhem, S., Linera, R., Seese, G., Martin, M., Vanderberg, N., Giordano, J., DeGennaro, P., Jonas, A.B. et al. (2016). White paper on bio-psycho-social applications to cognitive engagement. Technical Report, Defense Technical Information Center.

Zhang, Y. & Wildemuth, B.M. (2009). Qualitative analysis of content. In Applications of social research methods to questions in information and library science, 308(319), pp. 1–12.