Widening CyBOK: A Mapping of Strategic & Defence Cyber Research against the Knowledge Areas

Final Report delivered by Professor Basil Germond, Lancaster University
23 October 2024

Executive summary

- Scholars in the field of strategic, defence and security studies have only engaged with CyBOK in a limited way.
- The aim of this project is to assess the extent to which current CyBOK Knowledge Areas (KAs) are relevant to scholars in this field, to identify the limitations of existing KAs and to suggest avenues for enhanced engagement with CyBOK resources.
- 134 academic articles in the field have been mapped against current KAs to identify compatibility and discrepancies.
- The findings show that a few existing KAs are relevant to studies in the field (in particular 'Adversarial Behaviours') but that scholars in the field would benefit from an elaboration of the descriptors of some KAs and sub-topics of KAs to better include issues related to cyber operations in a military/war context.
- Additionally, findings show that scholars in the field would benefit from the development of a new KA (or sub-topics of KAs) or a Supplementary Guide that would offer a detailed account of cyber capabilities and applications in the context of war as well as of key trends in the field, such as critical national infrastructures, the cyber 'grey zone', and the role of the private sector as an agent of cyber warfare (both as adversaries and partners).
- The recommendations for CyBOK are those of the author and are made to generate debates within the CyBOK community. CyBOK is not endorsing any particular view. There is a change request process if changes to CyBOK are to be formally proposed.

Introduction

The need to better account for the importance of the social science dimensions of cyber security is well-documented (ENISA, 2018; Pirta-Dreimane et al., 2022). Yet, the extent to which CyBOK Knowledge Areas (KAs) cover the wider range of social science cyber security research is still limited (Carpent & Furnell, 2023: 1). This is particularly salient in the sub-field of strategic, defence and security studies (within the field of International Relations). Addressing this gap would amplify the KAs' value for many researchers in the field, whose contributions to the body of knowledge could potentially be significant, especially in an era of geopolitical tensions, systemic volatility, and increasing military confrontations.

CyBOK's strength is its scope as "an evolving knowledge base" (Catal et al., 2023: 1811), which is "for the community, by the community" (Rashid, 2021). And as KAs become more widely disseminated, it is expected that they will be "challenged and developed" (Martin and Collier, 2021). Against this backdrop, the aim of this study is to determine the compatibility of existing CyBOK KAs (and relevant sub-topics of KAs) with research in the field of strategic, defence and security studies and, when gaps are identified in current KAs' coverage, to suggest additions or revisions to existing KAs to increase their relevance for research in the field.

This report is divided into two parts. The first part presents the mapping of the body of knowledge in the field of strategic, defence and security studies against the existing CyBOK KAs. This constitutes the main academic outcome of the project. Then, based on the findings from the mapping exercise, the second part of the report suggests avenues for researchers in strategic, defence and security studies to engage in a meaningful way with existing CyBOK KAs as well as recommendations to the CyBOK community on a potential expansion of the scope and coverage of KAs.

Part 1. Mapping strategic, defence and security research against the Knowledge Areas

1.1. Framework for analysis

Despite some initial ontological reluctance in the 1990s and early 2000s to engage with 'cyber' as an object distinct from 'information warfare' (Zilincik and Duyvesteyn, 2023), strategic, defence and security studies have offered an important prism of analysis of cyber threat, cyber war and, more broadly, cyber security by using and applying accepted concepts originating in realist IR theories (Cavelty and Wenger, 2020; Cristiano et al., 2023). In particular, the concept of 'cyber power', i.e. actors' ability to use digital technologies and the cyber space to maximize and/or enact power, has been coopted by traditional strategic and defence studies (Zilincik and Duyvesteyn, 2023). In practice, cyber-attacks, cyber defence, cyber conflicts, cyber war, and cyber warfare are frequent objects of study in the field of strategic, defence and security studies, whether mentioned in passing or as the main focus (e.g., Burton, 2015, 2018, 2022; Burton and Christou, 2021).

However, there is, to date, no CyBOK KA specifically dedicated to the above-mentioned topics and issues. Additionally, none of the existing CyBOK Supplementary Guides is dedicated to them. The 'Risk Management & Governance' KA addresses 'risk governance' and 'security policy' but not in a way compatible with the ontology of strategic studies. Indeed, the approach is focused on 'best practices' to address cyber risks and threats and not on cyber defence policies. The 'Law & Regulation' KA addresses issues related to public international law and thus states' involvement in cyber operations, including during armed conflicts. However, the focus of this KA is on *jus ad bellum* (i.e. cyber-attacks, like 'traditional' forms of use of force against another sovereign state, are usually prohibited) and *jus in bello* (i.e. in case of war, accepted principles must be adhered to such as proportionality, discrimination, military necessity, etc.). These questions are of importance to IR scholars in general but they are not central to inquiries in strategic, defence and security studies, although the ethics of cyber warfare is a topic of growing concern within the community; indeed, cyber warfare induces moral considerations that are inherent to war and warfare and, in particular, to cyber war and cyber warfare, since the normative framework is developing at a slower pace than the related technologies and their applications. The 'Adversarial Behaviours' KA is the closest to address questions of war and defence, but the scope of existing discussions of state actors' adversarial behaviours is limited to 'sabotage', 'espionage', and 'disinformation'. This covers relevant activities studied by strategic, defence and security scholars but falls short of offering a detailed enough framework for the analysis of war and warfare in the cyber age. The same limitations apply to the 'Cyber Physical Systems' KA that covers cyber conflicts and state behaviours indeed but focusing mainly on definitions and legal considerations and not much on the use of cyber capabilities during conflicts.

This research postulates that we can expand CyBOK KAs, and specifically the 'Adversarial Behaviours' Knowledge Tree v.1.0.1, to better account for the defence dimension of cyber security and respond to strategic, defence and security studies' ontological needs. The approach is thus deductive, at least in its initial phase. Yet, the data was approached without preconception: the research was driven by data and when the body of research examined fitted with the existing KAs, the approach was iteratively modified to make room for an inductive discussion of how researchers in the field can better engage with existing KAs.

1.2. Methodology and data processing

This project employs a proven method for the mapping and transversal analysis of complex relationships between research areas and analytical frameworks: a two-stage quantitative-qualitative review of the literature in a specific sub-field (Germond, Hindley and Brennan, 2024; Montoya et al., 2019). A recent study in *Computer Science Review* demonstrates this method's relevance for a cognate project on research communities in cyber security (Katsikeas et al., 2021).

Data was collected in the form of peer-reviewed journal articles in the field of strategic, defence and security studies and cognate disciplines and sub-fields using the *Web of Science* abstract and citation database, which is recognised (along with *Scopus*) as the most comprehensive yet selective multidisciplinary academic citation indexes (Martín-Martín et al., 2018). To collect relevant articles, an initial search was conducted in 'All fields' with the keywords 'cyber security' or 'cyber conflict', or 'cyber warfare', or 'cyberwar'. This returned 15,845 token (see Table 1).

Table 1: Number of articles before and after data cleaning

	Number of articles
All returns for initial keyword search	15,845
Filtered grand total (before cleaning)	299
Sub-total (after manually removing handbooks)	168
Sub-total (after manually removing false positive and non-available articles)	134

Then, the following filters were applied: type of document = articles; categories = International Relations or Political Science; Language = English; Research areas = International Relations; Publication years = 2013-2023 (i.e. a 10-year span). This returned 299 tokens. Handbooks were then removed manually, resulting in a dataset of 168 academic articles. Finally, false positives (i.e. articles only mentioning cyber security in passing) and those unavailable via Lancaster University (where the research was conducted) were manually removed for a final sub-total of 134 articles.

These 134 articles were qualitatively analysed to identify themes and areas covered or not by existing CyBOK KAs. Three questions informed the mapping exercise:

> Q1: What field/sub-field of study does the article best align with?
>
> Q2: To which existing CyBOK KA(s) or sub-topics of KAs is the article related (if any)?
>
> Q3: What elements are missing from the existing KAs? Which new cyber areas would better reflect the article's focus?

For each of these three questions, articles were mapped using tags that were pre-identified based on the readings of a qualitatively representative sample of the dataset and then refined iteratively during the analysis. Table 2 presents the final list of tags for each of the three questions.

Table 2: Tagging

Disciplines	Existing KAs (and sub-topics of KAs)	Suggested new areas
-Critical security studies -Diplomacy and foreign Policy -Generic security studies -Intelligence studies -International law -National security -Security policy -Terrorism studies -War and strategy	-Adversarial Behaviours Disinformation Espionage Sabotage -Cyber Physical Systems -Risk Management & Governance Risk communication Enacting security policy -Human Factors -Law and Regulation Ethics Jurisdictions Jus ad bellum *Jus in bello*	-Critical national infrastructures -Cyber defence and cyber war -Cyber diplomacy -Cyber discourse and securitization -Cyber geopolitics -Cyber policy -Cyber power -Cyber terrorism -Grey zone -International cooperation and governance structures -Psychological warfare -State violence -Strategic thinking -The politics of science, technology, and innovation -Weapons and AI

While processing the row data (articles) and creating the dataset, each article was tagged with one primary discipline, but then tagged to zero, one, or more existing KA(s) and zero, one, or more suggested new area(s). This resulted in the creation a 166-pathway dataset linking disciplines in the field with existing KAs and suggested areas. The dataset was analysed by focusing on each of the three questions and then via transversal analyses of the complex interlinkages between subject areas (disciplines), existing KAs/sub-topics of KAs and proposed areas. The outcome is a comprehensive mapping of the compatibility of strategic, defence and security studies with existing KAs.

Findings are limited to the knowledge generated via this (necessarily) limited analytical exercise. In particular, the qualitative analysis of each article could only be conducted at a high scale due to the limited scope of this project. Consequently, some more subtle links and connections might have been overlooked during the data processing phase. However, there is a strong confidence in the relevance of the highlighted links.

1.3. Findings

1.3.1. Findings in relation to disciplines (Q1)

Out of all the articles in the dataset, the most represented discipline is 'Generic security studies', followed by 'War and strategy', 'National security', and 'Diplomacy and foreign policy'. Altogether, sub-disciplines directly related to defence, war, and strategy account for 43% of the articles and more generic security and IR studies for 42% (see Table 3).

Table 3: Most represented sub-disciplines

Disciplines	%
Generic security studies	23,17%
War and strategy	22,76%
National security	18,29%
Diplomacy and foreign Policy	13,82%
Critical security studies	8,54%
Security policy	4,88%
International Law	4,88%
Intelligence studies	2,03%
Other dimensions	1,22%
Terrorism studies	0,41%
Total	**100,00%**

Interestingly, 8.54% of the articles (21) have been tagged as 'Critical security studies'. Critical security studies is a sub-field of security studies that applies critical theories and approaches to challenge and expand traditional, so-called mainstream, security concepts and focuses on questions of securitization and ethics. Findings demonstrate a serious engagement of this sub-field of security studies with cyber and defence questions. Indeed, cyber operations, especially offensive ones as well as the governance of the cyber space are topics of interests to critical IR scholars. These articles are related to the following existing KAs and sub-topics of KAs (in descending order): 'Risk Communication' (KA Risk Management & Governance), 'Disinformation' (KA Adversarial Behaviours), 'Ethics' (KA Law & Regulations), 'Adversarial Behaviours', 'Risk Management & Governance', and 'Law & Regulation' (Table 4).

Table 4: Existing KAs or sub-topics of KAs relevant for 'critical security studies'

Existing KAs or sub-topics of KAs (Q2) for 'Critical security studies' (Q1)	%
n/a	28,57%
Risk communication	19,05%
Disinformation	14,29%
Ethics	14,29%
Adversarial Behaviours	9,52%
Risk Management & Governance	9,52%
Law & Regulation	4,76%
Total	**100,00%**

In fact, the main focus of critical security studies is the way cyber threats and cyber operations are represented or constructed in political (and security) discourses, i.e. the discursive process of securitization and its practical, policy consequences (e.g., surveillance, exceptional measures). In terms of suggested KAs (Q3), 43% of these studies (and 50% of those linked to none of the existing KAs that accounts for 29%) were tagged to the suggested area of 'cyber discourse and securitization', which is thus a relevant area to consider for further expansion of existing KAs.

Disciplines most associated with traditional defence studies (i.e. 'National security' and 'War and strategy') were mostly related to the existing KA 'Adversarial Behaviours' (including sub-topics 'sabotage', 'espionage', and 'disinformation') and to the KA 'Cyber Physical Systems' (see Table 5).

Table 5: Existing KAs and sub-topics of KAs relevant for traditional defence studies

Existing KAs or sub-topics of KAs (Q2) for combined 'National security' and 'War and strategy' (Q1)	%
n/a	29,70%
Adversarial Behaviours	20,79%
Sabotage	11,88%
Espionage	7,92%
Disinformation	4,95%
Cyber Physical Systems	10,89%
Risk Management & Governance	6,93%
Risk communication	0,99%
Law & Regulation	0,99%
Ethics	2,97%
Jus in bello	0,99%
Human factors	0,99%
Total	**100,00%**

This can be explained by the fact that these two KAs are those that account for the practice of disinformation, sabotage, and espionage, i.e. to the practice of *cyber operations*, which are the main object of study of the articles in the field of 'National security' and 'War and strategy'. It is also noticeable that almost 30% of these studies were not associated to any existing KA. Moreover, 50% of these studies (including 43% of those not linked to any existing KAs) would benefit from a new 'Cyber defence and cyber war' knowledge area (Table 6). This demonstrates the need to reflect on the absolute necessity to work on this particular area despite the relevance of two existing KAs.

Table 6: Suggested new areas for traditional defence studies

Suggested KAs or sub-topics of KAs (Q3) for 'National Security and 'War and Strategy' (Q1)	%
Cyber defence and cyber war	50,00%
Grey zone	8,33%
Challenges posed by private actors	7,29%
Critical national infrastructures	6,25%
Cyber power	6,25%
Cyber geopolitics	4,17%
Strategic thinking	4,17%
Weapons and AI	4,17%
Cyber discourse and securitization	3,13%
Cyber policy	2,08%
Psychological warfare	2,08%
International cooperation and governance structures	1,04%
The politics of science, technology and innovation	1,04%
Total	**100,00%**

Other beneficial new areas would be 'Grey zone' (8%), 'Challenges posed by private actors' (7%), 'cyber power' and 'critical national infrastructure (both 6%). Each of them would offer a focus on some specific, yet crucial, aspects of the use of cyber capabilities during conflicts/war operations in the 21st century.

Articles belonging to the category 'Generic security studies' (including 'Security policy') return similar results: 'Adversarial Behaviours' (and 'Disinformation', 'Espionage', and 'Sabotage') account for 63% of relevant existing KAs. This means that even for sub-disciplines less focused on cyber war/warfare these questions are central. Interestingly, non-security disciplines such as 'Diplomacy and foreign policy' highlight the importance of 'Risk Management & Governance' and 'Law & Regulation' (including 'Jurisdictions' and '*Jus in bello*') (50%) to which we can add 'Cyber Physical Systems' that accounts for similar issues (31%). For all studies that are more generic International Security than 'War and strategy', the suggested new KAs/sub-topics of KAs are 'Cyber defence and cyber war', 'Grey zone' and 'Challenges posed by private actors' (that mirrors what studies specialized on defence and strategy would also benefit from) but also more generic International Relations areas, such as 'International cooperation and governance structures', and 'Cyber discourse and securitization'.

1.3.2. Analysis focusing on existing KAs (Q2)

Given the above findings, it comes as no surprise that the existing KAs that are most relevant for strategic, defence and security studies are 'Adversarial Behaviours' and 'Cyber Physical Systems', including 'Disinformation', 'Espionage', and 'Sabotage' (Table 7). These are indeed the main subject areas of much of the dataset. Additionally, it is interesting to note that 10% of the articles relate to the KA 'Risk Management & Governance' and about 14% (combined) to the KA Law & Regulation and its sub-topics. This accounts for the need to regulate and govern the militarisation and weaponization of cyber capabilities.

Table 7: Most relevant existing KAs and sub-topics of KAs

Existing KAs and sub-topics of KAs	**%**
Adversarial Behaviours	22,46%
Disinformation	7,49%
Espionage	8,56%
Sabotage	11,23%
Cyber Physical Systems	14,44%
Risk Management & Governance	10,16%
Risk communication	2,67%
Enacting security policy	1,07%
Law & Regulation	5,88%
Ethics	5,88%
Jus in bello	3,74%
Jurisdictions	3,21%
Jus ad bellum	2,14%
Human factors	1,07%
Total	**100,00%**

Studies that align with KAs 'Adversarial Behaviours' and 'Cyber Physical Systems' would still benefit from the development of a KA focusing strongly on 'Cyber defence and cyber war' (41%) and one on

‘Grey zone’ (13%). Studies aligning with the KA ‘Risk Management & Governance’ would benefit from the development of the following new areas: ‘International cooperation and governance structures’ (44%) that would be more focused on the role of interstate cooperation and international organizations in governing the military application of cyber capabilities, ‘Challenges posed by private actors’ (28%) and ‘cyber discourse and securitization’ (17%). Studies aligning with none of the existing KAs would mainly benefit from a new area on ‘Cyber defence and cyber war’ (25%), which confirms the importance of cyber warfare considerations.

1.3.3. Analysis focusing on suggested new KAs or sub-topics of KAs (Q3)

The suggested new areas (see Table 8) have been defined qualitatively and iteratively (during the analysis). The most frequent ones are 1) ‘Cyber defence and Cyber war’ (which includes questions of cyber deterrence, the elaboration of cyber strategies, escalation, cyber weapons, cyber warfare, and what constitutes a military threat), 2) ‘The challenges posed by private actors’ (both as adversaries/proxies/threats and as partners for governments working with private actors (PPPs) – this also includes the ethical and legal implications of private companies participating in cyber defence and attack as well as the difficulty to attribute responsibilities), 3) ‘Cyber discourse and securitization’ (i.e. what is ‘cyber’ in the context of defence, what is constructed as ‘cyber’ and as a ‘threat’ and what are the practical consequences of such constructions, including the relation between ‘power’ and the construction of knowledge), 4) The ‘Grey zone’ (including hybrid warfare and ‘below-the-threshold’ operations, jurisdictional fuzziness, responsibilities and attribution), 5) ‘International cooperation and governance structures’ (including the role of international organizations), 6) ‘Cyber power’ (and the question of maximizing one’s power in/via the cyber space), and 7) ‘Critical national infrastructures’ (including energy security and communication). Less frequent/more niche suggested areas are ‘Cyber geopolitics’, ‘Cyber policy’, ‘Strategic thinking’ (and strategic thought on cyber),’The politics of science, technology and innovation’, ‘Weapons and AI’ (including the militarization of AI[1] for, among others, intelligence gathering, large data analysis, speed of decision-making, and targeting, as well as, more generally, the non-anthropogenic nature of cyber war), ‘Psychological warfare’ (and information warfare), ‘State violence’, ‘Cyber terrorism’, and ‘Cyber diplomacy’.

Table 8: Suggested new areas in descending order

Suggested areas	Number
Cyber defence and cyber war	70
Challenges posed by private actors	26
Cyber discourse and securitization	23
Grey zone	23
International cooperation and governance structures	23
Cyber power	13
Critical national infrastructures	9
Cyber geopolitics	7
Cyber policy	7
Strategic thinking	7
The politics of science, technology and innovation	7
Weapons and AI	6

[1] In particular: “the advantage of AI/ML approaches is that they may discover new successful attack pathways from the huge set of possible combinations” (Rhode, 2023: 7).

Psychological warfare	5
State violence	3
Cyber terrorism	2
Cyber diplomacy	1
Total	**232**

Looking at the suggested KA 'Cyber defence and cyber war' (which is prominent – 30%), the existing KAs that fit better with it are 'Adversarial Behaviours' and 'Cyber Physical Systems', which corroborates the above-mentioned results and demonstrates that a good option would be to strengthen these two existing KAs to make sure that they properly cover topics of interests to strategic, defence and security studies. The same findings emerge when looking at 'Grey zone' and 'Critical national infrastructures' with 'Adversarial Behaviours', 'Sabotage' and 'Espionage' being the existing KAs/sub-topics of KAs mostly associated with articles focusing on the grey zone and critical infrastructures and thus in need of more elaboration. Finally, for the suggested area 'Challenges posed by private actors', no existing KA stands out. In fact, this topic addresses a wide array of questions from governance to adversarial behaviours and from ethics and morality to law. This demonstrates the need to develop a new sub-topic of the KA Law & Regulation specifically devoted to the topic of private actors.

In case of articles where existing KAs cover enough (i.e. when there is no Q3 associated), the most prominent existing KAs/sub-topics of KAs are 'Cyber Physical Systems' and 'Disinformation'. This finding points towards the need to further elaborate on the strategic and defence studies dimension of these two KAs, although this is based on a small n (=18/134) and thus only elaborating existing KAs is unlikely to be sufficient.

1.4. Transversal analysis and discussion of findings

Data shows that articles in the field of strategic, defence and security studies are often within the scope of existing KAs and sub-topics of KAs. This is far more than expected at the start of this project. There are relatively few occurrences of articles for which no existing KA matches at all (39/134). This demonstrates that there is no major ontological discrepancy in the current CyBOK knowledge base. 27% of the articles for which no existing KA matches would benefit from a new KA devoted to 'Cyber defence and cyber war' but, among the others, many would benefit from very specific new sub-topics of KAs such as 'Grey zone', 'Cyber discourse and securitization', 'Cyber power', and 'Weapons and AI' (Table 9).

Table 9: Suggested KAs or sub-topics of KAs when no existing relevant KA(s) were identified

Suggested KAs or sub-topics of KAs	**%**
Cyber defence and cyber war	26,99%
Cyber discourse and securitization	11,11%
Grey zone	11,11%
Cyber power	7,94%
Weapons and AI	7,94%
Challenges posed by private actors	6,35%
International cooperation and governance structures	6,35%
The politics of science, technology and innovation	6,35%
Cyber policy	4,76%
Critical national infrastructures	3,17%

Strategic thinking	3,17%
Cyber diplomacy	1,59%
Cyber geopolitics	1,59%
Psychological warfare	1,59%
Total	**100,00%**

Yet even though existing KAs demonstrate a high degree of relevance, they often only reflect one part of the issue under scrutiny. For instance, ‘Adversarial Behaviours’ often fits with the overall discussion of cyber operations, cyber war, cyber power, and grey zone activities, but the discussions of espionage, disinformation, sabotage, and other forms of attacks are limited to short paragraphs in the existing KAs’ descriptors. Thus, despite the relevance of some core existing KAs (‘Adversarial Behaviours’ and ‘Cyber Physical Systems’ in particular), the military/strategic/defence dimensions of these areas are not detailed enough and would require more substance to be relevant for scholars in the field. In other words, it is not the ontology that is problematic, but the limited information and substance provided in the existing body of knowledge.

Additionally, ‘Adversarial Behaviours’ seems to be written as if only adversaries and disruptors were engaged in activities such as espionage and sabotage. However, in an era of increasing geopolitical competition, the collective West is also active in the cyber domain (both in a reactive and proactive way). Thus, KAs also need to account for the literature discussing how the West uses cyber capabilities to conduct defensive and offensive operations in defence of our interests and values.

Following the inception of internet and the first discussions of cyber war in the 1990s, the practice and academic discussions of cyber security have been dominated by commercial, private, and criminal (for-profit) considerations. And overall, the focus on military considerations is still a new academic endeavour (Zittrain, 2017). Since it is during these two decades that ideas for the CyBOK KAs have been matured, this can explain the lack of KAs focusing purely on more military aspects of cyber security. Surely, the preponderance of scholars from technical, science backgrounds in the CyBOK community has also played a role.

Furthermore, as shown above, some existing KAs can be further developed but some important new areas must also be considered in order to offer a comprehensive picture of the military/national security/defence dimensions of cyber security. Indeed, new developments have emerged such as the role of proxies and private (often for-profit) actors in support of state adversaries, responsible cyber power, the cyber ‘grey zone’, and critical national infrastructures. Such topics cannot be covered by expanding existing KAs only; indeed although KAs have been conceived in a “non-orthogonal way”, there is a limit to their transversal nature, and the above-mentioned issues would benefit from the existence of a specifically devoted KA or a Supplementary Guide.

Part 2. Recommendations

The outcome of this project consists in two sets of recommendations: some suggestions for researchers in strategic, defence and security studies to foster their engagement with existing KAs and with the CyBOK community in general, and some suggestions to the CyBOK community to make the body of knowledge more accessible and useful to scholars in the field.

2.1. Suggestions for researchers in strategic, defence and security studies

The CyBOK knowledge base provides an unparalleled source of information about all aspects of cyber security that is presented in a concise but comprehensive and transversal way. Yet, its overall focus is on the non-military dimensions of cyber security, which explains the relative lack of visibility of CyBOK within the strategic, defence and security scholarly community. Yet, for those researching the military/defence/strategic dimensions of cyber security, there is much to gain from engaging with CyBOK. Indeed, the complexity of the cyber ontology (multi/trans-domain, post-territorial and post-jurisdictional) requires scholars to rely on robust and trustworthy models, concepts and knowledge about all aspects of cyber security, from human and institutional behaviours to regulatory frameworks to technology. Below are some suggestions for researchers in strategic, defence and security studies.

2.1.1. State adversarial behaviours

The 'Adversarial Behaviours' KA has a section on state actors that covers espionage, sabotage, and disinformation. Not only is this KA a useful source of information but it is also possible to engage with the rest of the document that focuses on crime and criminal behaviours. Although state actors follow a different business model, their operating model can be very similar to those of criminals, or they can even act in a coordinated way.

2.1.2. International law

The 'Law & Regulation' KA has short sections on jurisdiction, public international law, and ethics that surveys many of the questions raised in the literature interested in cyber war, cyber conflicts and cyber operations. The 'Cyber Physical Systems' KA has a section on 'Cyber conflict', which mentions cyber terrorism and offensive cyber activities by states and link them to legal considerations, including the law of armed conflicts. Similarly to 'Adversarial Behaviours', the contextualization provided by these two KAs (beyond their discussion of elements relevant to cyber warfare) is invaluable in the quest to address the issues of ontological complexity.

2.1.3. Critical security studies

Scholars in this sub-field should engage with sub-topics of KAs related to 'Risk communication', 'Disinformation', and 'Ethics' that are closely related to questions of securitization and the discourse on cyber security that scholars in this sub-field deconstruct. Indeed, the way, risks are communicated is a form of discourse, i.e. a narrative that represents what the threats are and what the solutions should be, which then has an impact on actors' practices. Similarly, disinformation as a cyber activity is core to questions of democracy, ethics, and attribution that are the subjects of critical security studies. Thus, scholars in critical (cyber) security can engage with existing KAs either as a source of information or as material they can use to analyse and deconstruct the existing narrative about cyber security.

2.1.4. Core war and strategic studies

As shown above, none of the existing KA is specifically devoted to questions of weapons, warfare, and military strategy. Yet, scholars in these fields are encouraged to look at the entire supply chain of the KA, using the main tree and its various sub-trees. Indeed, many existing KAs help structuring one's understanding of the many interrelated and complex mechanisms that affect, constrain, and enable cyber operations, whether threat perception, risk assessment, communication, adversarial behaviours, technology, regulatory frameworks, ethics, attribution, human factors, etc. In other words, CyBOK (as a knowledge base) offers an extensive source of information for scholars in war and strategic studies that can help bringing order to the complex ontology of cyber security. A holistic approach to cyber will also contribute to addressing recurring questions about the relevance of the concept of 'cyber war' itself given its conceptual flaws (Zilincik & Duyvesteyn, 2023).

2.2. Recommendations to the CyBOK community[2]

This project has shown that there are two possible avenues to make CyBOK more accessible and relevant to strategic, defence and security studies scholars. These two avenues can be pursued in isolation or in combination.

2.2.1. Further elaborating existing KAs

One way to make CyBOK more relevant for scholars in this field is to further elaborate some existing KAs (and sub-topics of KAs). It would be possible to strengthen the existing KAs 'Adversarial Behaviours' and 'Cyber Physical System' in order for them to better cover the subject matter of strategic, defence and security studies, namely cyber war, cyber warfare, military strategies and cyber operations. For instance, it would certainly be easy to further elaborate on espionage, sabotage, and disinformation. Similarly, for the KA 'Law & Regulation', there is more to say about *jus in bello* in practice in relation to actual operations and future risks; also the sub-topics of KA 'Ethics' needs to be framed within discussions of cyber operations and the responsible use of cyber capabilities during war. Such incremental additions to the KAs are easy to implement and would make a huge difference for scholars in the field.

2.2.2. Developing new KAs/sub-topics of KAs or a Supplementary Guide

Another suggestion is to develop a new major KA on 'Cyber warfare'. Such a new KA would delve into the various dimensions of cyber war and warfare, including (but not limited to) cyber operations during war, cyber tactics, strategy and doctrines, the military use of offensive and defensive cyber capabilities, *jus in bello*, cyber weapons, the use of AI on the battlefield). Additionally, sub-topics of KAs specifically devoted to some areas identified as important are needed, especially on critical national infrastructures, the cyber grey zone, and the role of private actors. An alternative way forward, given that cyber warfare permeates through many existing KAs and sub-topics of KAs, could be to develop a Supplementary Guide focusing on cyber war and cyber warfare.

Conclusion

The aim of this project was to identify avenues for a better engagement of the strategic, defence and security studies scholarly community with CyBOK. Both the need to account for the militarization of cyber security in the past decades and the opposite calls for demilitarizing cyber conflicts (Boeke & Broeders, 2018) necessitate scholars in the field to engage with the comprehensive body of knowledge that CyBOK offers that transcends military considerations. Findings presented in Part 1 point in two directions:

[2] The recommendations for CyBOK are those of the author and are made to generate debates within the CyBOK community. CyBOK is not endorsing any particular view. There is a change request process if changes to CyBOK are to be formally proposed.

1) Existing KAs are more relevant than thought during the design phase of the project. For scholars in the field, it is thus worth making the effort to engage with relevant existing KAs and for the CyBOK community, it would be worth exploring ways to further elaborate the military/warfare dimensions of some existing KAs to make them more relevant and palatable to researcher in this field.

2) Results also show that there is a need to develop new KAs or Supplementary Guide to better reflect the evolution of the scholarship on cyber security that has increasingly engaged with questions of war, warfare, and military operations, including critiques of the relevance of 'cyber war' and the effectiveness of cyber operation during conflicts (e.g., Maschmeyer & Dunn Cavelty, 2022), as well as with the cyber grey zone and the cyber agency of private actors during war.

This project has demonstrated that both parties will gain from more engagement: strategic, defence and security scholars by broadening their intellectual horizon in order to manage the complex ontology of cyber security and ”overcome the institutional barriers that slow down interdisciplinary and more so transdisciplinary research” (Dunn Cavelty and Wenger, 2020: 26); and the CyBOK community by strengthening its knowledge base, making it more relevant to a group of scholars and a type of studies that are going to be increasingly important given the geopolitical context.

References[3]

Boeke, S., & Broeders, D. (2018). The Demilitarisation of Cyber Conflict. *Survival*, *60*(6), 73-90.

Burton, J. (2022). The Future of Cyber Conflict Studies. *The Cyber Defense Review*, *7*(3), 103-116.

Burton, J. (2018). Cyber deterrence: A comprehensive approach?. *NATO Cooperative Cyber Defence Centre of Excellence*, https://ccdcoe.org/library/publications/cyber-deterrence-a-comprehensive-approach/.

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. *Defence Studies*, *15*(4), 297-319.

Burton, J., & Christou, G. (2021). Bridging the gap between cyberwar and cyberpeace. *International affairs*, *97*(6), 1727-1747.

Cristiano, F., Kurowska, X., Stevens, T., Hurel, L. M., Fouad, N. S., Cavelty, M. D., ... & Shires, J. (2023). Cybersecurity and the politics of knowledge production: towards a reflexive practice. *Journal of Cyber Policy*, 1-34.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

Germond, B., Hindley, J. & Brennan, J. (2024). The impacts of climate change on maritime security and ocean sustainability. *Global Challenges in Maritime Security: Sustainability and the Sea*. Otto, L. & Menzel, A. (eds.). Springer.

Katsikeas, S., Johnson, P., Ekstedt, M., & Lagerström, R. (2021). Research communities in cyber security: A comprehensive literature review. *Computer Science Review*, *42*, 100431.

[3] These are the references to the articles quoted in this report. For a list of the articles that constitute the project's database, see appendix 1 below.

Martin, A., & Collier, J. (2020). Beyond awareness: Reflections on meeting the inter-disciplinary cyber skills demand. In *Cyber Security Education* (pp. 55-73). Routledge.

Martín-Martín, A., Orduna-Malea, E., Thelwall, M., & López-Cózar, E. D. (2018). Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories. *Journal of informetrics*, *12*(4), 1160-1177.

Maschmeyer, L., & Dunn Cavelty, M. (2022). Goodbye cyberwar: Ukraine as reality check. *CSS Policy Perspectives*, *10*(3).

Montoya, F.G. Alcayde, A. Baños, R. and Manzano-Agugliaro F. (2018). A fast method for identifying worldwide scientific collaborations using the Scopus database. *Telematics and Informatics*, *35*(1), 168-185.

Rashid, A. (2021). Opening up the world of cyber security: How the online landscape calls for increased knowledge. *Bristol Engineering Blog*, https://engineering.blogs.bristol.ac.uk/opening-up-the-world-of-cyber-security-how-the-online-landscape-calls-for-increased-knowledge/.

Rhode, M. (2023). *AI for Security Topic Guide Issue 1.0.0.*. CyBOK, https://www.cybok.org/media/downloads/AI_for_Security_TG_v1.0.0.pdf.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, *104*, 333-339.

Zilincik, S., & Duyvesteyn, I. (2023). Strategic studies and cyber warfare. *Journal of Strategic Studies*, *46*(4), 836-857.

Zittrain, J. (2017). "Netwar": The unwelcome militarization of the Internet has arrived. *Bulletin of the Atomic Scientists*, *73*(5), 300-304.

Appendix 1: <u>List of articles constituting the source for the cleaned database</u>

1. Abbasi, A. (2020). Hybrid War Threats and Essence of Perception Management: Challenges for Pakistan. *IPRI journal, XX (2), 1*, *24*.

2. Abramson, Y., & Baram, G. (2024). Saving face in the cyberspace: responses to public cyber intrusions in the Gulf. *Contemporary Security Policy*, *45*(2), 210-238.

3. Adamsky, D. (2017). The israeli odyssey toward its national cyber security strategy. *The Washington Quarterly*, *40*(2), 113-127.

4. Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083-1097.

5. Akoto, W. (2022). Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies. *Conflict Management and Peace Science*, *39*(3), 311-332.

6. Allenby, B. R. (2015). The paradox of dominance: The age of civilizational conflict. *Bulletin of the Atomic Scientists*, *71*(2), 60-74.

7. Ashraf, C. (2021). Defining cyberwar: towards a definitional framework. *Defense & Security Analysis*, *37*(3), 274-294.

8. Babb, C., & Wilner, A. (2019). Passwords, pistols, and power plants: An assessment of physical and digital threats targeting Canada's energy sector. *International Journal*, *74*(4), 518-536.

9. Bachmann, S. D., & Jones, M. (2021). Syria–a hybrid war case study. *Journal of Military and Strategic Studies*.

10. Baker-Beall, C., & Mott, G. (2022). Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis. *JCMS: Journal of Common Market Studies*, *60*(4), 1086-1105.

11. Ball, D., & Waters, G. (2013). Cyber defence and warfare. *Security challenges*, *9*(2), 91-98.

12. Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.

13. Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *44*(2), 147-164.

14. Boeke, S., & Broeders, D. (2018). The demilitarisation of cyber conflict. *Survival*, *60*(6), 73-90.

15. Boer, L. J. (2019). Lex Lata comes with a Date; or, What Follows from Referring to the "Tallinn Rules".

16. Bowers, I. (2018). The use and utility of hybrid warfare on the Korean Peninsula. *The Pacific Review*, *31*(6), 762-786.

17. Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization*, *75*(1), 39-70.

18. Brenner, J. F. (2013). Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the atomic scientists*, *69*(5), 15-20.

19. Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261-1280.

20. Brown, J. M., & Fazal, T. M. (2021). # SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security*, *6*(4), 401-417.

21. Buchan, R. (2016). Cyber warfare and the status of anonymous under international humanitarian law. *Chinese Journal of International Law*, *15*(4), 741-772.

22. Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble?. *Marine policy*, *155*, 105772.

23. Burton, J., & Christou, G. (2021). Bridging the gap between cyberwar and cyberpeace. *International affairs*, *97*(6), 1727-1747.

24. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

25. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

26. Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor?. *JCMS: journal of common market studies*, *55*(6), 1254-1272.

27. Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111-1126.

28. Choi, S. A., & Namkung, G. (2013). State-led Back-scratching Alliance in Cyber Warfare. *The Korean Journal of International Studies*, *11*(2), 295-325.

29. Choi, S. A., & Namkung, G. (2013). State-led Back-scratching Alliance in Cyber Warfare. *The Korean Journal of International Studies*, *11*(2), 295-325.

30. Chuanying, L. (2023). Forging stability in cyberspace. In *Survival: Global Politics and Strategy (April-May 2020)* (pp. 125-135). Routledge.

31. Cimbala, S. J. (2017). Nuclear deterrence and cyber warfare: coexistence or competition?. *Defense & Security Analysis*, *33*(3), 193-208.

32. Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, *72*(4), 234-237.

33. Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia's battle for cybersecurity norms. *Contemporary Security Policy*, *36*(2), 346-368.

34. Der Derian, J. (2022). Quantum espionage: a phenomenology of the Snowden affair. *Intelligence and National Security*, *37*(6), 920-936.

35. Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2022). The rise of cyber power in Brazil. *Revista Brasileira de Política Internacional*, *65*, e013.

36. Dortmans, P. J., Thakur, N., & Ween, A. (2015). Conjectures for framing cyberwarfare. *Defense & Security Analysis*, *31*(3), 172-184.

37. Dowling, M. E. (2021). Democracy under siege: Foreign interference in a digital era. *Australian Journal of International Affairs*,

38. Dowling, M. E. (2022). Foreign interference and Australian electoral security in the digital era. *Australian Journal of International Affairs*, *76*(1), 40-56.

39. Drezner, D. W. (2019). Technological change and international relations. *International Relations*, *33*(2), 286-303.

40. Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105-122.

41. Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

42. Dylan, H., & Maguire, T. J. (2023). Secret intelligence and public diplomacy in the Ukraine War. In *Survival: August-September 2022* (pp. 33-74). Routledge.

43. Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law*, *112*(4), 583-657.

44. Egloff, F. J. (2020). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, *41*(1), 55-81.

45. Egloff, F. J., & Shires, J. (2023). The better angels of our digital nature? Offensive cyber capabilities and state violence. *European journal of international security*, *8*(1), 130-149.

46. Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. *International Studies Perspectives*, *17*(3), 343-360.

47. Fouad, N. S. (2022). The non-anthropocentric informational agents: Codes, software, and the logic of emergence in cybersecurity. *Revie*

48. Garcia, D. (2016). Future arms, technologies, and international law: Preventive security governance. *European Journal of International Security*, *1*(1), 94-111.

49. Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International security*, *38*(2), 41-73.

50. Gill, A. S. (2019). Artificial intelligence and international security: the long view. *Ethics & International Affairs*, *33*(2), 169-179.

51. Gjesvik, L., & Szulecki, K. (2023). Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. *European Security*, *32*(1), 104-124.

52. Gomez, M. A. N. (2019). Sound the alarm! Updating beliefs and degradative cyber operations. *European Journal of International Security*, *4*(2), 190-208.

53. Gompert, D. C., & Libicki, M. (2014). Cyber warfare and Sino-American crisis instability. *Survival*, *56*(4), 7-22.

54. Gompert, D. C., & Libicki, M. (2023). Towards a quantum internet: post-pandemic cyber security in a post-digital world. In *Survival february–march 2021: A house divided* (pp. 113-124). Routledge.

55. Goychayev, R. (2016). On international cooperation in nuclear and cyber security. *Peace Review*, *28*(2), 220-229.

56. Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284-291.

57. Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK?. *European Security*, *22*(1), 21-35.

58. Hare, F. B. (2019). Precision cyber weapon systems: An important component of a responsible national security strategy?. *Contemporary security policy*, *40*(2), 193-213.

59. Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, *45*(4), 534-567.

60. Huang, K., Madnick, S., Choucri, N., & Zhang, F. (2021). A systematic framework to understand transnational governance for cybersecurity risks from digital trade. *Global Policy*, *12*(5), 625-638.

61. Jensen, B., Valeriano, B., & Maness, R. (2020). Fancy bears and digital trolls: Cyber strategy with a Russian twist. In *Military Strategy in the 21st Century* (pp. 58-80). Routledge.

62. Jiang, C. Decoding China's Perspectives on Cyber Warfare'(2021). *Chinese Journal of International Law*, *20*, 257-302.

63. Johnson, J. (2022). Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age. *European Journal of International Security*, *7*(3), 337-359.

64. Junio, T. J. (2013). How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. *Journal of Strategic Studies*, *36*(1), 125-133.

65. Kania, E. B., & Costello, J. (2021). Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power. *Journal of Strategic Studies*, *44*(2), 218-264.

66. Katagiri, N. (2024). Artificial Intelligence and Cross-Domain Warfare: Balance of Power and Unintended Escalation. *Global Society*, *38*(1), 34-48.

67. Kaufmann, M. (2016). Exercising emergencies: Resilience, affect and acting out security. *Security Dialogue*, *47*(2), 99-116.

68. Kennedy, A. B. (2023). The Resilience Requirement: Responding to China's Rise as a Technology Power. *Survival*, *65*(1), 115-128.

69. Kim, S. (2014). Cyber security and middle power diplomacy: A network perspective. *The Korean Journal of International Studies*, *12*(2), 323-352.

70. Kostyuk, N., & Brantly, A. (2022). War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation. *Contemporary Security Policy*, *43*(3), 498-515.

71. Kostyuk, N., & Gartzke, E. (2024). Fighting in cyberspace: Internet access and the substitutability of cyber and military operations. *Journal of Conflict Resolution*, *68*(1), 80-107.

72. Kritsiotis, D. (2013). Enforced equations. *European Journal of International Law*, *24*(1), 139-149.

73. Levin, A., & Goodrick, P. (2013). From cybercrime to cyberwar? The international policy shift and its implications for Canada. *Canadian Foreign Policy Journal*, *19*(2), 127-143.

74. Liebetrau, T. (2022). Cyber conflict short of war: a European strategic vacuum. *European Security*, *31*(4), 497-516.

75. Liebetrau, T., & Christensen, K. K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European journal of international security*, *6*(1), 25-43.

76. Liff, A. P. (2013). The proliferation of cyberwarfare capabilities and interstate war, redux: Liff responds to Junio. *Journal of Strategic Studies*, *36*(1), 134-138.

77. Lilli, E. (2021). Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence. *Contemporary Security Policy*, *42*(2), 163-188.

78. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404.

79. Lindsay, J. R. (2014). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7-47.

80. Lindsay, J. R. (2021). Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem. *Intelligence and National security*, *36*(2), 260-278.

81. Lupovici, A. (2021). The dual-use security dilemma and the social construction of insecurity. *Contemporary Security Policy*, *42*(3), 257-285.

82. Maďar, T. (2019). Lagging colossus or a mature cyber-alliance. *Obrana a strategie*, *19*(1), 5-22.

83. Malone, E. F., & Malone, M. J. (2013). The "wicked problem" of cybersecurity policy: analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal*, *19*(2), 158-177.

84. Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. *International Security*, *46*(2), 51-90.

85. Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, *46*(3), 570-594.

86. Maurushat, A. (2013). From cybercrime to cyberwar: security through obscurity or security through absurdity?. *Canadian Foreign Policy Journal*, *19*(2), 119-122.

87. McGuffin, C., & Mitchell, P. (2014). On domains: Cyber and the practice of warfare. *International Journal*, *69*(3), 394-412.

88. Meyer, P. (2015). Seizing the diplomatic initiative to control cyber conflict. *The Washington Quarterly*, *38*(2), 47-61.

89. Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review*, *15*(1), 86-104.

90. Neilsen, R. (2023). Coding protection:‘cyber humanitarian interventions’ for preventing mass atrocities. *International Affairs*, *99*(1), 299-319.

91. Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111-130.

92. Nye Jr, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future?. *Bulletin of the Atomic Scientists*, *69*(5), 8-14.

93. Osawa, J. (2017). The escalation of state sponsored cyberattack and national cyber security affairs: Is strategic cyber deterrence the key to solving the problem?. *Asia-Pacific Review*, *24*(2), 113-131.

94. Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, *5*(2), 233-254.

95. Petersen, K. L. (2020). Three concepts of intelligence communication: awareness, advice or co-production?. In *Intelligence on the Frontier Between State and Civil Society* (pp. 7-18). Routledge.

96. Peterson, D. (2013). Offensive cyber weapons: construction, development, and employment. *Journal of Strategic Studies*, *36*(1), 120-124.

97. Poornima, B. (2022). Cyber threats and nuclear security in India. *Journal of Asian Security and International Affairs*, *9*(2), 183-206.

98. Poznansky, M., & Perkoski, E. (2018). Rethinking secrecy in cyberspace: the politics of voluntary attribution. *Journal of Global Security Studies*, *3*(4), 402-416.

99. Rasheed, M. R., & Naseer, M. (2021). Digital Disinformation & domestic disturbance: Hostile cyber-enabled information operations to exploit domestic issues on Twitter. *IPRI Journal*, *21*(02), 95-129.

100. Rid, T. (2013). Cyberwar and peace: Hacking can reduce real-world violence. *Foreign Affairs*, *92*(6), 77-87.

101. Rid, T. (2013). More attacks, less violence. *Journal of Strategic Studies*, *36*(1), 139-142.

102. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1-2), 4-37.

103. Ross, C. L. (2024). Going nuclear: The development of American strategic conceptions about cyber conflict. *Journal of Strategic Studies*, *47*(1), 92-115.

104. Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy*, *34*(1), 40-63.

105. Saran, S. (2016). Striving for an international consensus on cyber security: lessons from the 20th century. *Global Policy*, *1*(7), 93-95.

106. Schaefer, D. (2024). Spies and scholars in the cyber age: researching intelligence in Australian policy and regional security. *Australian Journal of International Affairs*, *78*(1), 102-122.

107. Schneider, J., Schechter, B., & Shaffer, R. (2023). Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation. *International Organization*, *77*(3), 633-667.

108. Scully, T. (2016). Cyber security and the 2016 defence white paper. *Security Challenges*, *12*(1), 115-126.

109. Segal, A. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists*, *69*(5), 38-45.

110. Shah, M. A. (1986). Cyber Compellence: An Instrument of Technology-Driven Strategy. *Culture*, *27*(3), 544-560.

111. Shandler, R., Gross, M. L., & Canetti, D. (2021). A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. *Contemporary Security Policy*, *42*(2), 135-162.

112. Sharma, M. (2021). Modeling Attribution of Cyber Attacks Using Bayesian Belief Networks. *Strategic Analysis*, *45*(1), 18-37.

113. Shires, J. (2024). Career connections: transnational expert networks and multilateral cybercrime negotiations. *Contemporary Security Policy*, *45*(1), 45-71.

114. Shore, J. J. (2015). An obligation to act: Holding government accountable for critical infrastructure cyber security. *International Journal of Intelligence and CounterIntelligence*, *28*(2), 236-251.

115. Siroli, G. P. (2018). Considerations on the cyber domain as the new worldwide battlefield. *The International Spectator*, *53*(2), 111-123.

116. Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy*, *35*(3), 468-486.

117. Smeets, M. (2022). A US history of not conducting cyber attacks. *Bulletin of the Atomic Scientists*, *78*(4), 208-213.

118. Smith, F., & Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, *71*(6), 642-660.

119. Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*, *41*(1), 129-152.

120. Stevens, T. (2018). Cyberweapons: Power and the governance of the invisible. *International Politics*, *55*, 482-502.

121. Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5), 1079-1105.

122. Stone, J. (2013). Cyber war will take place!. *Journal of strategic studies*, *36*(1), 101-108.

123. Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy*, *40*(3), 368-381.

124. Tor, U. (2017). 'Cumulative deterrence'as a new paradigm for cyber deterrence. *Journal of Strategic Studies*, *40*(1-2), 92-117.

125. Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347-360.

126. Whyte, C. (2020). Beyond tit-for-tat in cyberspace: political warfare and lateral sources of escalation online. *European Journal of International Security*, *5*(2), 195-214.

127. Whyte, C. (2023). Learning to trust Skynet: Interfacing with artificial intelligence in cyberspace. *Contemporary Security Policy*, *44*(2), 308-344.

128. Whyte, J. (2022). Cybersecurity, race, and the politics of truth. *Security Dialogue*, *53*(4), 342-362.

129. Willett, M. (2023). The cyber dimension of the Russia–Ukraine War. In *Survival: October-November 2022* (pp. 7-26). Routledge.

130. Wirtz, J. J. (2017). Life in the "Gray Zone": observations for contemporary strategists. *Defense & Security Analysis*, *33*(2), 106-114.

131. Wolff, J. (2024). The role of insurers in shaping international cyber-security norms about cyber-war. *Contemporary Security Policy*, *45*(1), 141-170.

132. Zaighum, Z. & Rasool, F. (2023). Fifth-Generation Hybrid Warfare in Pakistan: Mapping Hybrid Threats, State Interpretation, and the Way Forward. *IPRI Journal*, 23(1), 53-78.

133. Zilincik, S., & Duyvesteyn, I. (2023). Strategic studies and cyber warfare. *Journal of Strategic Studies*, *46*(4), 836-857.

134. Zittrain, J. (2017). "Netwar": The unwelcome militarization of the Internet has arrived. *Bulletin of the Atomic Scientists*, *73*(5), 300-304.