CyBOK

The Cyber Security Body Of Knowledge

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

Professor Basil Germond

Lancaster University

contact@cybok.org
www.cybok.org

Outline

- Rationale for this study
- Methodology
- Findings
- Discussion
- Q&A

Rationale for this study (1)

- Strategic, defence and security studies scholars have only engaged with CyBOK in a limited way
- ‘Defence’ considerations are sparingly covered by existing KA and not in a way that respond to the ontological needs of scholars in the field (cyber operations)
- **Project aim**: To assess the relevance of existing KAs for defence studies, to identify gaps within existing KAs, and to suggest avenues for enhanced engagement with CyBOK resources
- Timely research: The contribution of ‘defence’ scholars to the body of knowledge could be significant in an era of geopolitical tensions, systemic volatility, and increasing military confrontations

Methodology (1)

- Data was collected in the form of peer-reviewed journal articles in the field of strategic, defence and security studies using the Web of Science abstract and citation database
- 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. Disciplinary and other filters were applied, resulting in a final dataset of 134 articles

	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

Methodology (2)

- These 134 articles were qualitatively analysed to identify themes and areas covered or not by existing CyBOK KAs, informed by three questions:
  - **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

Methodology (3): Tagging

- Each article was tagged with one primary discipline, then tagged to 0, 1, or more existing KA(s) and to 0, 1, 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**

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

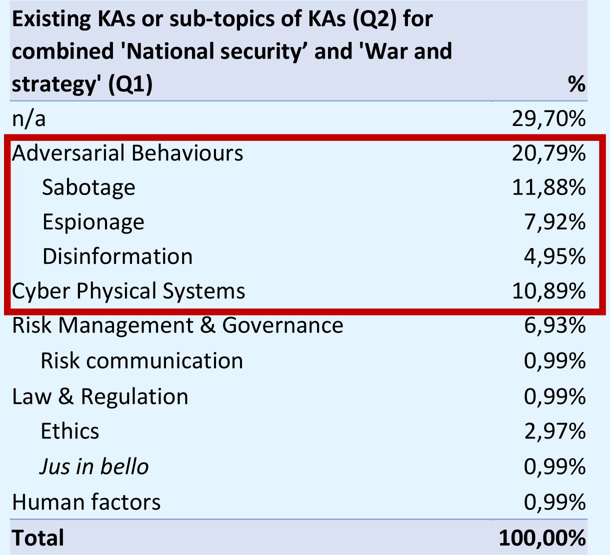
CyBOK

Findings (1): Most represented disciplines

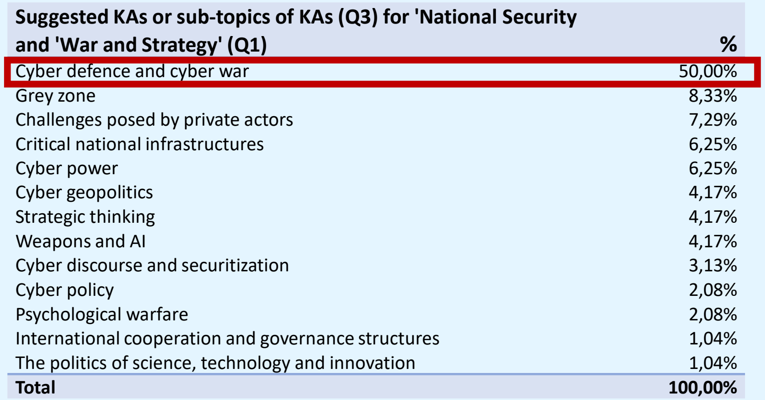
Disciplines	%
Generic security studies	23,17%
War and strategy	22,76%
National security	18,29%
Diplomacy and foreign Policy	13,82%
Critical security studies	8,54%
Security policy	4,88%
International Law	4,88%
Intelligence studies	2,03%
Other dimensions	1,22%
Terrorism studies	0,41%
Total	**100,00%**

Findings (2) Defence Studies

- Traditional **Defence studies** are mostly related to the existing **KAs 'Adversarial Behaviours' and 'Cyber Physical Systems'**
- Because these two KAs account for the practice of **disinformation, sabotage, and espionage, i.e. cyber operations** = the main object of study in the dataset
- 30% of these studies were not associated to any existing KA
- 50% of these studies **would benefit from a new 'Cyber defence and cyber war' KA**



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%**



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%**

Findings (3): Critical Security Studies

- 8.54% of the articles have been tagged as '**Critical Security Studies**'
  - A sub-field of security studies that applies critical theories to challenge and expand traditional security concepts and focuses on questions of securitization and ethics
  - Cyber operations and governance of the cyber space are topics of interests to critical IR scholars: How are cyber threats and cyber operations represented in political (and security) discourses, how does it normalize policies (e.g., surveillance, exceptional measures)?
- The relevant existing KAs or sub-topics of KAs for CSR are **'Risk communication', 'Disinformation', and 'Ethics'**
- 43% of these studies were tagged to the **suggested area of 'cyber discourse and securitization'**

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%**

Findings (4): Most relevant existing KA

Relevance of 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%**

- ‘**Adversarial Behaviours**’ and ‘**Cyber Physical Systems**’, including ‘Disinformation’, ‘Espionage’, and ‘Sabotage’

  = Cyber ops

- 10% of the articles relate to the KA ‘**Risk Management & Governance**’ and about 14% (combined) to the KA **'Law & Regulation**’ and its sub-topics

  = Regulation and governance of the militarization and weaponization of cyber capabilities

- Studies aligning with none of the existing KAs would, unsurprisingly, mainly benefit from a new area on ‘Cyber defence and cyber war’ (25%)

Findings (5): Suggested new areas

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

- ‘Cyber defence and cyber war’ is a serious candidate for a new KA (30%)
- The existing KAs that fit better with it are ‘Adversarial Behaviours’ and ‘Cyber Physical Systems’
- An option would be to strengthen these two existing KAs to make sure that they properly cover topics of interests to defence studies

CyBOK

Findings (8): Need for a new KA?

- Data shows that articles in the field of defence studies are often within the scope of existing KAs and sub-topics of KAs
- This is far more than expected at the start of the project - **There is no major ontological discrepancy in the current CyBOK knowledge base**
- Yet even though existing KAs demonstrate a high degree of relevance, they often only reflect one part of the issue under scrutiny
- **It is not the ontology that is problematic, but the limited information and substance provided in the existing body of knowledge**

Suggestions for researchers in defence studies

- Defence scholars are encouraged to **look at the entire supply chain of the KA**, using the main tree and its various sub-trees
- This will help structuring their understanding of the many **interrelated and complex mechanisms that affect, constrain, and enable cyber operations**: threat perception, risk assessment and communication, disinformation, adversarial behaviours, technology, regulatory frameworks, ethics, attribution, human factors
- 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**

What the CyBOK community can do

- **Further elaborating existing KAs**
  - ‘Adversarial Behaviours’ and ‘Cyber Physical System’ could better cover the subject matter of defence studies, namely cyber war, cyber warfare, military strategies and cyber operations
  - ‘Law & Regulation’ could say more about *jus in bello* during actual operations and future risks; The sub-topics of KA ‘Ethics’ could include discussions of cyber operations and the responsible use of cyber capabilities during war
- **Developing new KAs or a Supplementary Guide**
  - A new major KA on ‘Cyber warfare’ would delve into the various dimensions of cyber war and warfare, including 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**