IMSISS Dissertation Feedback & Mark Sheet

Student Matriculation No.	**Glasgow** 2685539 **DCU** 21109621 **Charles** 85545841
Dissertation Title	The Ukraine cyber war: an analysis of the Russian cyber doctrine for comparing the Ukraine National Cyber Security Strategy with those of other western countries

Word Count Penalty *(1-15% over/under = 1gr point; 15-20% over/under = 2 gr points; 20-25% over/under = 3 gr points; more than 25% over/under = 0 fail)*		
Word Count: 21986 ***Suggested Penalty:*** *Select from drop down list*		

JOINT GRADING (subject to agreement of the external examiner and approval at Joint Exam Board)

Final Agreed Mark : A4 [19]

DISSERTATION FEEDBACK

Assessment Criteria	***Rating***
A. Structure and Development of Answer This refers to your organisational skills and ability to construct an argument in a coherent and original manner	
• *Originality of topic*	Excellent
• *Coherent set of research questions and/or hypothesis identified*	Excellent
• *Appropriate methodology and evidence of effective organisation of work*	Very Good
• *Logically structured argument and flow of ideas reflecting research questions*	Excellent
• *Application of theory and/or concepts*	Very Good
B. Use of Source Material This refers to your skills to select and use relevant information and data in a correct manner	
• *Evidence of reading and review of published literature*	Excellent
• *Selection of relevant primary and/or secondary evidence to support argument*	Excellent
• *Critical analysis and evaluation of evidence*	Excellent
• *Accuracy of factual data*	Very Good
C. Academic Style This refers to your ability to write in a formal academic manner	
• *Appropriate formal and clear writing style*	Very Good
• *Accurate spelling, grammar and punctuation*	Excellent
• *Consistent and accurate referencing (including complete bibliography)*	Excellent
• *Is the dissertation free from plagiarism?*	Yes

IMSISS Dissertation Feedback & Mark Sheet

• *Evidence of ethics approval included (if required based on methodology)*	Yes
• *Appropriate word count*	Yes

ADDITIONAL WRITTEN COMMENTS

Reviewer 1

The master's thesis deserves recognition for its extensive study and in-depth analysis. The thesis is divided into two main parts: a detailed examination of formal doctrine documents and a comprehensive technical analysis of Russian hacker groups, affiliating them with major Russian intelligence, military, or law enforcement agencies.

The author's meticulous research and mapping of Russian hacker groups provide valuable insights into Russian cyber offensive capabilities. This not only contributes to the existing body of literature on the subject but also has practical implications, offering recommendations to enhance the cyber security of NATO members. By studying the cyber security doctrines of Ukraine, in comparison to key Western states such as the US, France, and Germany, the author highlights important similarities and differences that provide a broader perspective on the subject.

One of the notable parts of the thesis is the inclusion of interviews with experts in the cyber security field. This adds cutting-edge facts and perspectives that are not yet available in the literature, enriching the analysis and enhancing the thesis's value. However, it is acknowledged that conducting interviews during wartime may present challenges, and the limited scope of interviews could somewhat limit the analytical basis for drawing conclusions.

The master's thesis is further noted by its mixed methodology approach, which incorporates both qualitative and quantitative methods. This combination of research techniques allows the author to gain a more comprehensive understanding of the subject matter, drawing on the strengths of each approach.

The qualitative aspect of the study, which involves a detailed analysis of formal doctrine documents and expert interviews, provides valuable insights into the mindset and intentions behind Russian and Ukrainian cyber security doctrines. By delving into the text and conducting interviews, the thesis captures nuances and contextual information that quantitative data alone may not fully elucidate.

On the other hand, the quantitative component of the thesis, particularly in the technical analysis of Russian hacker groups, offers a systematic and objective perspective. The typology created to affiliate these groups with Russian intelligence, military, or law enforcement agencies demonstrates a structured and data-driven approach to understanding the cyber landscape.

However, it is important to acknowledge that mixing methodologies can be challenging and might lead to complexities in interpreting and synthesizing findings. Striking the right balance between qualitative and quantitative data requires careful consideration and could present limitations in terms of standardization and generalization of results.

In light of this mixed methodology, the thesis could benefit more from a clear and explicit explanation of how the qualitative and quantitative data complement each other and how potential conflicts or discrepancies between the two are reconciled. By simplifying the presentation of

methodological approaches and their integration, the thesis could enhance its accessibility and clarity for readers, making it easier to grasp the overall findings and implications.

The inclusion of a mixed methodology in the study enables a multifaceted examination of Russian and Ukrainian cyber security doctrines. Nonetheless, it would be helpful to provide a concise and transparent explanation of how these methods harmonize to address potential complexities and ensure the study's coherence.

In summary, the master's thesis makes a contribution to the study of Russian and Ukrainian cyber security doctrines, demonstrating the author's dedication to rigorous research and analysis. The practical recommendations provided in the thesis offer real-world applications for improving cyber security, and the incorporation of expert interviews adds depth to the research. The thesis can serve as a valuable resource for academics, policymakers, and practitioners interested in cyber security and international relations. To strengthen future research, it could be beneficial to widen the scope of interviews and continue to incorporate diverse and up-to-date sources in times of conflict.

Reviewer 2

The opening clearly outlined the study's significance and originality. The work was also very well situated in relation to the literatures around Russian cyberwarfare and those studies specific to the comparisons of cyber security strategies of the different countries being considered. The approach adopted and potential limitations were similarly identified. There could have occasionally been scope further to reflect on the methodologies employed, although these were more clearly articulated during the course of the research.

The work is very good at providing a systematic anatomy of different Russian cyber threats and groups involved. Careful consideration is given to the implications of different actors involved and the cross-country comparative dimension. The quantitative analyses were very useful in providing scope for greater comparison of the respective threat landscapes. Interviews provided some effective insights into contemporary perceptions regarding cybersecurity policies in the context of the War in Ukraine.

Charting of strategies by different countries provided interesting insights into their respective public conceptualising of cyber 'threats' and the problematic nature of definitions in forming their approaches (including that of 'critical national infrastructure'). There was effective analysis of the range of sources and contemporary material through these different sections and chapters.

The framework for scoring cyber resilience was very interesting, including in charting the presence of references/strategies in policy documents as an indicator of awareness. However, some of the otherwise useful conclusions arising from this could have been qualified. For instance, it could have been beneficial further to have reflecting on the points around the extent to which resilience and awareness are linked to the respective capabilities identified or aspired to through the documents.

It could similarly have been helpful to have developed the reflections on the extent to which the absence of naming potential threats or naming 'strategies' in certain contexts may have been for other reasons than lack of awareness/strategy, such as the possibility references to hostile organisations or threats in particular cases may be classified or deliberately kept away from

IMSISS Dissertation Feedback & Mark Sheet

official documents.

The dissertation was well presented, including in its structure. Selective rewording of sentences would enhance this. A range of reading was used in support of points and conclusions provided a useful summary of the main arguments.

A well-researched and effective dissertation, original in its comparative approach and topic, engaging in focused interweaving of sources and analysis. It could be enhanced by some development of points, but otherwise makes a valuable contribution to this topical area around Ukraine Cyber Warfare and global implications.