



## Diploma Thesis Evaluation Form

Author: **André Viana**

Title: **NATO and Offensive Cybersecurity: A Strategic Analysis**

Programme/year: **2018**

Author of Evaluation (supervisor/external assessor): **Raluca Csernaton, PhD**  
Postdoctoral Researcher & Lecturer  
Institute of Political Studies (IPS)  
[raluca.csernaton@fsv.cuni.cz](mailto:raluca.csernaton@fsv.cuni.cz)

| Criteria              | Definition                                  | Maximum    | Points |
|-----------------------|---|------------|--------|
| <b>Major Criteria</b> |   |            |        |
|                       | Research question, definition of objectives | <b>10</b>  | 9      |
|                       | Theoretical/conceptual framework            | <b>30</b>  | 24     |
|                       | Methodology, analysis, argument             | <b>40</b>  | 35     |
| <i>Total</i>          |   | <b>80</b>  | 68     |
| <b>Minor Criteria</b> |   |            |        |
|                       | Sources                                     | <b>10</b>  | 10     |
|                       | Style                                       | <b>5</b>   | 5      |
|                       | Formal requirements                         | <b>5</b>   | 5      |
| <i>Total</i>          |   | <b>20</b>  | 20     |
| <b>TOTAL</b>          |   | <b>100</b> | 88     |



## Evaluation

**Major criteria:** The research puts forward an impressive handle of the subject matter, offering a thorough understanding of both the empirical dimension and the academic scholarship dedicated to NATO's recent cyber security strategy. Its main contribution is that it opens up for investigation and testing three conceptual lenses from the Strategic Studies scholarship, namely punctuated deterrence, cyber persistence, and cyber deception, in order to formulate potentially valid cybersecurity strategies for NATO regarding the use of offensive cyber capabilities. The value-added of the thesis is that it provides a comprehensive evaluation of the three selected concepts and the utility of offensive cyber capabilities for self-defence in the case of NATO. The assessment is based on their strategic value in accordance to the Lykke Model as suitable, feasible and theoretically acceptable for NATO. The research concludes that none of the three selected concepts leads to a valid strategy applicable to NATO, thus advancing knowledge about their theoretical strategic value to potentially articulate an effective operational strategy for NATO in the cyber domain.

**Minor criteria:** The thesis is very well written and structured, being indicative of good argumentation skills and a thorough handle of scholarly craft. From research question formulation, literature review, conceptual framework, and methodology, the thesis provides a well-balanced theoretical and conceptual analysis of the subject matter.

**Overall evaluation:** The author demonstrates an in-depth knowledge of the relevant scholarship dedicated to NATO's cybersecurity posture, raising interesting points during the analysis as regards the offense-defence theory, the risks associated with cyberspace, and the introduction of new cyber technologies in warfare. Its main contribution is that it opens up for investigation the value of offensive cyber capabilities, analysed through three diverging conceptual lenses, for NATO's overall cybersecurity strategy.

Suggested grade: **1**

Signature: Prague, 28.08.2018