Appendix: Assessing Sweden's Current Cybersecurity Landscape: Implications of NATO Membership

Nike Henriksén[1], Isak Lexert[2], Jakob Bergquist Dahn[2] and Simon Hacks[1][a]

[1]*Department of Computer and System Sciences, Stockholm University, Stockholm, Sweden*
[2]*Halmstad University, Halmstad, Sweden*
{*nike.henriksen, isak.lexert56, jakob.b.dahn*}*@gmail.com, simon.hacks@dsv.su.se*

Keywords: Cybersecurity, Sweden, NATO membership, Cyber Defense, Cyber Threats.

Abstract: Sweden's recent NATO membership marks a significant shift in the country's national security strategy, particularly concerning cybersecurity. This study has assessed the current cybersecurity landscape in Sweden by conducting interviews with experts within the public sector and through document analysis. The interviewees included academics, researchers, and government officials from the municipal level to parliament. The study concludes how the threat environment has evolved following Sweden's NATO membership. The study has identified key cyber threats facing Sweden, primarily from state-sponsored actors such as Advanced Persistent Threat (APT) groups and cybercriminal organizations targeting critical infrastructure. The study has also found disparities in cybersecurity preparedness between Sweden's military and civilian sectors. The study emphasizes the need to strengthen civilian cybersecurity to reach a similar preparedness as the military to adapt to NATO's requirements and standards.

Interview Questions Group 1

1. What is your experience in cybersecurity (education, organization, area within the organization)?
2. How has the cyber threat against Sweden/your organization evolved recently?
3. How has Sweden's cyber defense developed over the past few years?
4. What does Sweden's cyber defense look like today?
5. Has there been any noticeable difference in the cyber threat since Sweden became a NATO member, or is there any indication that the cyber threat will increase?
6. How do you think NATO membership will impact the cyber threat against Sweden?
7. In what ways are Swedish authorities affected by cyber threats from state actors?
8. What do you think the future holds for Sweden regarding cyberattacks, cyber threats, and cyber defense?
9. Do you have any specific events or incidents your organization has experienced in this area that you can share?

Interview Questions Group 2

1. What does Swedish membership in NATO mean for national cybersecurity?
2. Is the threat landscape for Swedish cybersecurity affected before and after joining NATO? If yes, how?
3. Does Sweden receive support regarding cybersecurity from NATO? If yes, what kind of support and when?
4. Is Sweden expected to contribute to the alliance's cybersecurity? If yes, how?
5. How does NATO membership affect cybersecurity in your organization?
6. What threats do you consider most relevant regarding cybersecurity concerning NATO membership?
7. How have you adapted your cybersecurity strategy to meet the changing threat landscape with NATO membership?

[a] https://orcid.org/0000-0003-0478-9347

8. How should smaller individual organizations adapt their cybersecurity strategies to meet the changing threat landscape with NATO membership?
9. Do you feel the necessary measures before and after NATO membership differ between public and private sectors? Or other entities?
10. What measures have been or are the most important to implement to be prepared during the NATO accession?
11. Does NATO impose any cybersecurity requirements on Swedish companies and authorities? If yes, what are the requirements and for whom?
12. Do you perceive that NATO membership entails a greater threat for any specific entity?