Assessment Analysis of NATO cyber defense policy

Today, I will be doing an analysis of how Experts have assessed NATOs 2024 cyber defense policy and will be going over how these assessments may have led to additional implications for the policy. We will also be going over how I would assess NATOs cyber defense policy in order to achieve a lowered risk of implications within the policy itself, which would make the policy overall more appealing to the public. This paper going forward will be structured and organized in the following sections. Firstly we will be going over "how experts have evaluated this policy", "how those evaluations lead to more policy implications", "how i would assess this policy", and lastly the conclusion to wrap everything up. Now let us begin with our first section "how experts have evaluated this policy".

Now we will be going over 3 evaluations of NATOs cyber defense policy from experts. The first evaluations will be from Mario P Etthymiopoulos whose assessments about NATO'S cyber defense policies where that in order to ensure the success of this policy NATO would need to make sure that it is capable of preventing cybercrime from all levels and not just reacting to cyberattacks that have already happened. Meaning NATO needs to take pre emptive measures to ensure digital security amongst its member states and to do that would require the use of generative AI systems to find and secure potential cyber threats within networks(Sjs, 2024). He also mentioned that NATO would need to also address emerging hybrid and asymmetrical threats with this policy(Sjs, 2024).

Now the second evaluation of NATOs cyber defense policy I've looked at is from Jason Healey who wrote in his analysis that he praised how NATO is addressing the rise in cyber threats. He also mentions how NATO is making sure that the cyber security centre is leading the response to cyber attacks, which is good because of their technical expertise within the cybersecurity field(Council, 2019).

Finally for the last evaluation I'll be using today is from the FDD which goes on to say in their analysis that NATOs needs to focus on making sure that NATO’s NICC (integrated cyber center) is capable of planning and implementing cyber operations amongst its member states and the private sector as the whole purpose of the NICC is to provide a shared situational awareness for cyber defense and such must be a high priority of this new sub-group to ensure proper collaborations within the alliance within the cyber domain(Spaulding & Montgomery, 2024). Now that we have gone over some of the points from these evaluations let's now look at how these evaluations could lead to more implications for NATOS 2024 cyber defense policy.

Now with these evaluations of NATO'S cyber defense policy came with it some ethical, political, and social implications whether the authors of those papers realized it or not. So we will be breaking some of them down in order to shed light on some possible issues this policy may bring with it. First let's go back and look at the analysis from Mario P Etthymiopoulos. when reviewing his evaluation of the policy I noticed that it shed light on some political implications within the policy being its need to use generative AIs to help secure networks something that this policy is already looking to use to create a more fool proof security model but this leads to problems such as privacy and possible even the risk of over reliance of AI.

Now the ethical implications that had been brought to light by Jason Healey analysis of NATO's cyber defense policy was the reliance on defense to protect against cyber attacks and the need to acquire a greater degree of cyber offensive capabilities as one of NATOs founding principle is if on member states are attacked then all are, so NATO must have sophisticated offensive cyber capabilities to act on that principle if needed. But this also creates an ethical problem being whether or not going to digital war or even physical war over just cyber attacks is ethical.

Lastly, for the analysis from the FDD showed some social implications within the Policy, being an over reliance on the NICC to plan and conduct cyber operations as one of the main goals of the policy is to have help from the private sector. The NICC shouldn't be solely responsible for the planning of cyber operations when also being assisted by outside companies because that could lead to them not properly utilizing the experience and expertise they hope to use to help them create a stronger, more digitally secure NATO. Now let’s take a look at how I would assess this policy.

Firstly, when trying to assess the effectiveness of this policy we first need to establish the main points that this policy should be addressing in order to get the effect it was made to achieve, in this case a greater degree of cyber defense against both nation states and criminal actors. So what are the main points this policy should be addressing? Well it is risk assessment, management, Data protection, and incident response. While researching for NATO’s 2024 cyber defense policy I’ve determined that it adequately covers all of the main points listeds, so then if everything is already covered then what are its solutions to those problems? Well for risk assessment and management NATOs plans on using advanced AI to analyze and the use of a new sub-group within NATO called NICC to manage and address threats. For data protection the plan will be utilizing new advanced security systems alongside sophisticated AI systems to ensure all data is secure. Then lastly for incident response the policy plans to work together amongst its member states and private sectors to quickly contain, neutralize and patch any breaches that occurred. Overall I’d say that this policy is very well formulated to effectively respond and deal with the ever growing sophistications and rate of cyber attacks in our digital world, which will ensure that the people who live in NATO countries will be able to live peacefully without the constant worry of cyber attacks.

Now I don’t think that my assessment ended up removing the implications that this policy may face when its problematic aspects become more widely known to the public but I do think the way I framed the policy in a good light and as an effective and honest means of cyber defense for not only governments but the people too. Now lastly let’s go on to the conclusion of this paper.

In conclusion, this paper went over 3 different evaluations of NATO'S 2024 cyber defense policy from Mario P Etthymiopoulos, Jason Healey, and the FDD which all gave different and unique assessments of the policy but was generally accepted to be well formulated and focused on meeting NATO’s cyber security needs for not only itself but for its citizens as well. I also did my own assessment of the policy where I found that it addressed everything that a cybersecurity policy should, such as having a plan for implementation of risk assessment and management, Data protection, and incident response to ensure maximum security and integrity for its systems. Of course this policy also came with some political, ethical, and social implications that were brought to light by these assessments and even though I wasn't able to fully remove some of these implications with my own assessment I believe that overall the concerns that people may bring up will be quickly settled as everyone realises that it’s for the best digital protection possible for not only NATO but for the people too, in our ever growing digital world.

SOURCES

Council, A. (2019, April 9). *NATO cyber Defense: Moving past the summit - Atlantic Council*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-cyber-defense-moving-past-the-summit/?utm_source=chatgpt.com

Sjs. (2024, March 20). *NATO must adopt a pre-emptive approach to cyber security | GJIA*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture/

Spaulding, S., & Montgomery, R. M. (2024, July 10). NATO and Cyber: Outrunning the Bear. *FDD*. https://www.fdd.org/analysis/op_eds/2024/07/08/nato-and-cyber-outrunning-the-bear/?utm_source=chatgpt.com