NATO Cyber Defense Policy: A Political Breakdown

James F. Keith

CYSE425W: Cybersecurity Strategy and Policy

Professor Hamza Demirel

February 16, 2025

NATO Cyber Defense Policy: A Political Breakdown

According to Davis et al. (2021), “In 2021 NATO declared that cyberspace would be a new domain of warfare. Nations pledged to promote their own cyber defenses and various existing NATO means and measures were enhanced, including a NATO cyber range” (p. 153). While cyber defense is crucial to the security of all NATO members in today’s geopolitical landscape, NATO leaders did not consider this strategy necessary. It wasn’t until the cyberattacks on Estonia in 2007 that NATO realized the political and security implications cyber-based attacks could have on its members. According to Blessing et al. (2021), “After Estonia’s 2007 cyber incident, NATO members had a greater urgency to address cyberspace challenges and, in January 2008, approved an initial *Policy on Cyber Defense*” (p. 266).

Before the cyberattack on Estonia, few understood hybrid warfare and its implications. Most nations perceived hybrid warfare as adversaries utilizing propaganda or hysteria to instill panic or fear in another country’s population. However, Russian-sponsored attackers introduced a new form of hybrid warfare during the 2007 distributed denial-of-service (DDoS) attack on Estonia. According to Hardy and Robinson (n.d., as cited in Manjikian and Romaniuk, 2021), the relocation of a Soviet World War II memorial from downtown Tallinn to a less popular cemetery enraged Estonia’s Russian-speaking minority. Clashes erupted but were quelled on the same day. However, the next 23 days were filled with several waves of coordinated distributed denial-of-service (DDoS) attacks against Estonia’s government web pages, banks, and information systems (p. 212). The attacks are believed to have been undertaken by Russian government proxies but were considered a wake-up call for both NATO and Estonia. Hardy and Robinson (n.d., as cited in Manjikian and Romaniuk, 2021) stated the following:

> Two significant developments in 2008, in the immediate aftermath of the cyberattacks, point to such a trajectory. First was the prompt establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in the country's capital Tallinn the following summer. Not only was its formation incredibly symbolic, recognizing the country's established expertise in cybersecurity in light of Estonia's response to the 2007 attacks, but was also a clear indication from within the NATO alliance that Estonia could lead on issues pertaining to cyber defense and international law. (pp. 211-212)

Known as the "Bronze Night," all countries, including NATO members, quickly recognized the political significance of not having a cyber-based defense policy, viewing it as a national security threat. In Estonia, the government created its first National Cyber Security Strategy (2008-2013), laying the groundwork for formal cybersecurity measures and emphasizing the need to protect cyberspace (Hardy and Robinson, 2021, p. 213). NATO also acknowledged this issue and adopted the NATO Cyber Defense Policy at its 2008 Summit in Bucharest, Hungary.

According to Barna, et al. (2016), "Article 72 of the NATO Wales Summit Declaration states that: "Cyber-attacks impact could be as harmful to modern societies as a conventional attack"" (p. 151). The 2007 cyberattack on Estonia served as a wake-up call for all of NATO to ensure that each member's cyberspace was promptly secured. NATO leaders took the necessary steps to guarantee that the alliance would be ready to defend its members' cyberspace by emphasizing the significance of cybersecurity. Additionally, world leaders ensured that their respective countries established new rules and regulations for their cyberspace in anticipation of future cyberattacks. Although the Estonia cyberattack caused minor damage, the political implications were felt globally as countries reinforced their cybersecurity and implemented strategic measures to be prepared for future attacks.

References

Blessing, J., Elgin, K. K., Ewers-Peters, N. M., & Tiderman, R. (2021). NATO 2030: Towards a New Strategic Concept and Beyond (pp. 266-267). Brookings Institution Press. https://muse.jhu.edu/pub/11/oa_edited_volume/book/99306/pdf

Davis, G. D., Slobodchikoff, M. O., & Stewart, B. (2021). The Challenge to NATO (1st ed., p. 153). Potomac Books, Incorporated. Blessing, J., Elgin, K. K., Ewers-Peters, N. M., & Tiderman, R. (2021). NATO 2030: Towards a New Strategic Concept and Beyond (pp. 266-267). Brookings Institution Press. https://muse.jhu.edu/pub/11/oa_edited_volume/book/99306/pdf

Fortuna, A., Barna, C., & Iancu, N. (2016). *Countering Hybrid Threats: Lessons Learned From Ukraine* (1st ed., p. 151). IOS Press, Incorporated. https://ebookcentral.proquest.com/lib/odu/detail.action?pq-origsite=primo&docID=4605141

Hardy, A., & Robinson, N. (2021). *Routledge Companion Guide to Global Cyber-Security Strategy* (M. Manjikian & S. N. Romaniuk, Eds.) (1st ed., pp. 211-213). Routledge. https://www-taylorfrancis-com.proxy.lib.odu.edu/books/edit/10.4324/9780429399718/routledge-companion-global-cyber-security-strategy-mary-manjikian-scott-romaniuk