Risks to the Mission Partner Environment: Adversarial Access to Host Nation Network Infrastructure

Captain Kyle Sullivan

ABSTRACT

NATO's ability to communicate and win in the next conflict is based on the idea of Federated Mission Networking (FMN). The US initiative for the FMN is the Mission Partner Environment (MPE). This framework is built around the use of host nation network infrastructure. Recently, adversarial nations have been investing and developing host nation network infrastructure for NATO allies and partners. China, through companies such as Huawei, is leading the development of next-generation networking technologies. Russia has shown in recent conflicts that it will target a nation's network infrastructure to achieve its military goals. Russian political strategy is to expand its control over the strategic industries of countries in its sphere of influence. National network infrastructure will be considered strategic in the next conflict. Adversarial access to a host nation's network infrastructure threatens the MPE and NATO's ability to operate as a unified alliance. NATO must develop a strategy for a unified response by its member nations to protect their network infrastructures against unsecured network equipment of adversarial countries. NATO should also invest in options to provide secure communications for future mission partners which may have already sold control of their national network infrastructure to an adversary.

INTRODUCTION

At the 2014 Wales Summit, the North Atlantic Treaty Organization (NATO) passed the Connected Forces Initiative (CFI). This initiative set forth the goal of creating an interoperable force capable of operating alongside mission partners in any environment. The CFI implemented the idea of Federated Mission Networking (FMN), which provides the ability for ally and partner forces to communicate, train, and

Kyle Sullivan is currently a Captain in the U.S. Army Signal Corps and a graduate of the Joint Command, Control, Communications, Computers, and Intelligence/Cyber Staff and Operations Course (JC4ICSOC) at the National Defense University. He has a B.S in Computer Science as well as an M.S. in Cybersecurity from the University of Delaware. In his civilian life, he has worked as a software engineer at the Army's Software Engineering Center in Aberdeen Proving Grounds, Maryland, and holds professional certifications in cybersecurity. In the military, he has served in a variety of joint assignments where he implemented Mission Partner Environment communications alongside NATO allies in countries such as Croatia, Bosnia, Bulgaria, Hungary, Iraq, Italy, Romania, and Slovenia.

operate together.[1] The U.S.-based initiative for the FMN is called the Mission Partner Environment (MPE). The MPE is a network that enables information sharing by NATO allies and mission partners and creates unity of effort for mission forces down to the tactical level. In essence, the MPE is how NATO will perform Command, Control, Communications, Computers, and Intelligence (C4I) with its mission partners during future operations. A joint publication on Joint Communication Systems outlines how "the MPE is established using mission partner communications network infrastructure."[2] The MPE framework is therefore designed around the use of host nation network infrastructure for its success. However, in recent years adversarial nations have been investing in network infrastructure within NATO and partner countries.[3] Adversarial access to host nation network infrastructure poses several cybersecurity risks that threaten the MPE. These risks can degrade or deny NATO's ability to perform C4I during operations, which would severely impact the ability of the alliance to accomplish its mission. NATO and its partners must mitigate the cybersecurity risks to the Mission Partner Environment by working with host nations to reduce adversarial access to host nation network infrastructure.

China: The Red Team Dragon

As far back as the 1980s, the government of China identified telecommunications infrastructure to be strategically important and a source of technological strength.[4] Today, this strategic goal is still being pursued by China as made evident by the rise of Chinese companies which are investing in network infrastructure around the world. In recent months, Chinese-backed companies such as ZTE and Huawei have increased their efforts to expand in Europe, especially in the emerging 5G technology field.[5] Pressure by Chinese companies to build network infrastructure in Europe has gained enough momentum that it now "seems inevitable that [they] will build large portions of [the]

5G infrastructure – including for some of the US' closest allies."[6] As a result, the future of European network infrastructure is concerning given the influence of Chinese-based companies. This poses a risk to the MPE framework because the network infrastructure of European countries, many of which are NATO allies and partners, will be influenced and tied to China, which is a non-NATO nation.

While China is not a formally recognized adversary, the 2019 NATO Summit announced that "China has security implications for all allies,"[7] insinuating an adversarial-style role. The framework for MPE was designed with the use of host nation infrastructure in mind, but underneath is an inherent assumption that the host nation has control of the network. If a host nation loses control of its network infrastructure, it will compromise its ability to operate within the MPE. If a nation-state actor, such as China, can leverage access or control over a nation's network infrastructure, it could divide or isolate a NATO ally or partner, reducing the effectiveness of the alliance. In the worst-case scenario, an adversary could deny a NATO ally or partner access to the MPE. This would prevent that nation from information-sharing abilities and prevent it from being able to operate alongside mission partners as a unified force, ultimately undermining interoperability.

Currently, there has been a mixed response from NATO countries to the use of Chinese network equipment in national infrastructure.[8] Across the alliance there are differing opinions on how a nation should invest in and develop its network infrastructure. As a result, it remains unclear how secure the future backbone of the MPE will be from a meddling nation-state actor like China.

Russia: The Grey Hat Bear

Russia, a traditional adversary of NATO, has shown in recent conflicts that it is willing and able to disrupt network infrastructure of its adversaries and will leverage cyberattacks to further its goals. In the 2008 conflict with Georgia, Russia exploited Georgian communications by leveraging physical proximity to network infrastructure. This was because the national network infrastructure of Georgia ran through Russian territory, which allowed Russia access to launch cyberattacks and effectively control the host nation network.[9] Furthermore, Russia conducted military operations to cut fiber and disrupt other infrastructure across Georgia to deny Georgia the ability to communicate and force the use of Russian-controlled network infrastructure.

These strategies were employed once again a few years later in the 2014 conflict with Ukraine over the disputed territory of Crimea. During the Crimean conflict, Russian forces showcased their cyber capabilities and conducted cyberattacks on the Ukrainian power grid, demonstrating how powerful cyber effects can be.[10] These cyberattacks were not only aimed at Ukraine but also against various European organizations including NATO. At the start of the conflict, "various NATO websites were hit by denial-of-service attacks, and NATO servers were infected by the same malware that infected Ukrainian institutions."[11] These attacks could have been made as an effort to stop any NATO involvement during the conflict. During the Crimean annexation, Russia demonstrated the strategic advantage of targeting host nation network infrastructure. In the midst of the conflict, Russian forces conducted a military raid on Ukrainian network infrastructure during which they cut off Crimean communications and isolated them from the outside world.[12] Had Ukraine been a NATO ally during the conflict, its ability to operate within the MPE may have been denied. As a result, a unified NATO response to the Russian aggression would have been hindered as mission partners were isolated and unable to communicate. The effects of these cyberspace attacks grant Russia a clear strategic advantage during a future conflict. Russia continues to achieve these same strategic advantages before the onset of the next conflict through its ongoing political strategy across Europe.[13]

Russian strategy is to gain access or control of the national infrastructures in its sphere of influence, such as in the Baltics and the Balkans.[14] This access can enable Russia to compromise a nation's network infrastructure during a conflict, either through control of power generation (e.g., disrupting the power grid) or through physical proximity to network equipment allowing for exploitation. While Russia does not exercise the same economic influence that China does with developing and exporting network technologies, Russia has used the same strategies as China in recent years in its attempts to control host nation network infrastructure.

Based on reports by the US and allied cyber intelligence agencies, Russia has been discovered using hacking techniques to exploit network infrastructure devices across nations worldwide in attempts to seize key cyber terrain.[15] Once network devices are exploited, Russian hackers can remain in hiding and wait for a strategic opportunity to launch cyberattacks. These network device exploits conducted by Russian state-sponsored cyber actors achieve the same ultimate goal as pursued by Chinese companies such as Huawei, etc., to access and control a nation's network infrastructure. Russia has shown in past conflicts that it will target network infrastructure and, based on its current strategy, will continue to do so again in the future.

This threat is further amplified by closer relations between China and Russia. With the implementation of China's New Silk Road initiative in 2015, network infrastructure has been built directly between Russia and China to shield the two countries from US and Western intelligence agencies and further align the two nations.[16] With this in mind, it is not difficult to imagine that, at the start of a conflict with NATO, an adversary such as Russia would be quick to target and disrupt network infrastructure. In doing so, it would deny the ability of an invaded nation to communicate and operate on the MPE, thus preventing a unified NATO response.

Threats to Cyberspace: The Fifth Domain

As the physical world evolves into the cyberspace domain, it is increasingly true that "network equipment is now integral to the critical infrastructure of any country."[17] From a technological perspective, "the equipment vendors of these network infrastructures pose a real threat to national security."[18] If an adversary controls the network between two parties, it allows for a variety of attacks such as the Man-In-The-Middle attack (MITM).[19] Moreover, while cryptography technologies may protect the confidentiality of communications, MITM attacks can still allow for a variety of other malicious actions such as a denial-of-service attack.[20] Additionally, the strength of cryptography is always being tested, in which new methods such as "side channel attacks"[21] are emerging and prove to be extremely difficult to defend against.[22] With control over network infrastructure, an adversary would have access to critical information that could be leveraged for malicious means. With access to network base stations, which are primarily being installed by Huawei, an adversary would "possess a complete overview of where all mobile equipment is located, and thus, where all users are located."[23] This access could facilitate the leakage of sensitive information such as troop movements, which would provide vital military intelligence to an adversary. In addition to intelligence gathering, an adversary could "choose to turn off parts of the country's infrastructure or modify the infrastructure so it only works for their armed forces."[24] There are endless possibilities that an adversary could pursue if it controls network infrastructure.

All these threats are underlined by the fact that it is "way beyond feasible"[25] to analyze network equipment completely and verify it is secure. For a nation to trust the equipment in their network infrastructure fully, "the producer must remain trustworthy throughout the product's lifetime."[26] This means that using third-party equipment will always pose a risk to a nation's network infrastructure. These cybersecurity risks threaten the MPE and stand to undermine the interoperability of NATO.

Recommendations: An Interoperable NATO Response

The strategic importance of network infrastructure cannot be understated. Just as a nation protects its critical military equipment, so too must a nation protect its network infrastructure. NATO must make clear to all members that threats posed to network infrastructure not only impact the host nation itself but threaten the effectiveness of the alliance. NATO can use its political influence with member nations to ensure a unified response to using third-party network equipment such as that offered by Huawei. This can be accomplished through normal diplomatic means or by expanding the CFI at a subsequent summit to address using third-party equipment. At the very least, as NATO nations develop their mission networks, they need to identify critical segments of their network infrastructure and ensure only trustworthy equipment is being installed. While this may be possible in NATO countries, there will still be challenges with other mission partners which may not even be identified until a mission is already underway.[27] By the time a mission partner needs to operate within the MPE, its network infrastructure may already be controlled by an adversary. NATO must invest in flexible communications options that it can deploy to provide a secure networking backbone and enable the MPE in situations where the network infrastructure of a host nation is compromised. These flexible options could take the form of tactical mobile networking assets which are sourced from trustworthy producers and stockpiled before the next conflict.

CONCLUSION

NATO's Connected Forces Initiative outlines how it will use host nation network infrastructure to communicate and win in future conflicts with US allies and partners. Adversarial nations are vying for control and influence over strategic national network infrastructures. It is these network infrastructures that will be the backbone for the Mission Partner Environment and set the stage for future battlefields. NATO nations will have to align their political goals for national development with their strategic goals of protecting network infrastructure to ensure NATO remains an interoperable alliance. NATO can do this by enacting initiatives for member nations to identify strategic network infrastructure and develop them only by using trustworthy suppliers. For mission partners, NATO can stockpile secure network equipment to be deployed for use in contested network environments. Adversaries have demonstrated that they have the ability to access our networks, possess the technical skills, and that they lack the legal safeguards[28] to launch cyberattacks against NATO allies and partners. NATO must continue to defend strategic cyberspace terrain to ensure its greatest strength is preserved-interoperability. Through interoperability, members can act together coherently, effectively, and efficiently as an alliance, ensuring NATO will continue to guarantee the freedom and security of its members around the world.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. "FEDERATED MISSION NETWORKING," NATO, accessed March 15, 2020, https://www.act.nato.int/activities/fmn.
2. U.S. Department of Defense, "Joint Communication Systems," Joint Publication 6-0, October 4, 2019.
3 . The most prevalent example is China with its company Huawei; source: Lawrence Norman "Huawei Faces Deepening Scrutiny in Europe," *The Wall Street Journal*, Dow Jones & Company, January 31, 2019, https://www.wsj.com/articles/huawei-faces-deepening-scrutiny-in-europe-11548930489.
4. Deborah Brautigam, *The Dragon's Gift: The Real Story of China in Africa* (Oxford: Oxford University Press, 2011), 74.
5. 5G technology refers to the fifth generation of mobile networks which, in addition to faster communication speeds, intends to be the connectivity means of choice for various industries. These include automotive, health, public safety, armed forces, manufacturing, smart cities, and home automation.
6. Joseph Marks, "The Cybersecurity 202: The U.S. Is Going after Huawei, but It Isn't Changing Allies' Minds," *The Washington Post*, February 14, 2020.
7. Christopher Woody, "NATO Is Finally Talking about China, and There Are 3 Big Problems It Has to Address," *Business Insider*, December 12, 2019, https://www.businessinsider.de/international/china-poses-3-problems-in-europe-for-nato-2019-12/?r=US&IR=T.
8. Responses range from the United States outright banning Chinese companies such as Huawei, to Germany, UK, and France moving cautiously and taking a risk mitigation approach but still conducting business with Huawei. Some countries such as Italy, Austria, Poland, Estonia, and Lithuania, are undecided, while other NATO countries such as Spain and Slovakia are openly accepting Chinese investment and currently moving forward with Huawei equipment.
9. R.J. Deibert, R. Rohozinski, and M. Crete-Nishihata, Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war, *Security Dialogue*, 2012, 43(1), 3-24; doi:10.1177/0967010611431079.
10. Marie Baezner and Patrice Robin, "Cyber and Information Warfare in the Ukrainian Conflict," Center for Security Studies (CSS), October 2018, https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict.
11. Ibid.
12. Tony Martin-Vegue, "Are We Witnessing a Cyber War between Russia and Ukraine? Don't Blink You Might Miss It," *CSO Online*, April 24, 2015, https://www.csoonline.com/article/2913743/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html.
13. Russia implements its strategy via threats to gas supplies and acquiring energy or power assets across Europe. Sometimes Russian state-owned proxy companies acquire entire retail chains for energy products.
14. Stefan Ralchev, "Energy in the Western Balkans: A Strategic Overview," *Institute for Regional and International Studies*, August 2012, https://www.iris-bg.org/fls/Energy_in_the_Western_Balkans_Overview__Aug12.pdf.
15. Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, April 2018, retrieved August 2, 2020, https://us-cert.cisa.gov/ncas/alerts/TA18-106A?utm_source=newsletter.
16. N. Rolland, August 15, 2019, China's Belt and Road Initiative: Five Years Later, retrieved March 20, 2020, from https://www.nbr.org/publication/chinas-belt-and-road-initiative-five-years-later/.
17. Olav Lysne, Ahmed Elmokashfi, Niels Nagelhus Schia, Lars Gjesvik, and Karsten Friis, "Critical Communication Infrastructures and Huawei," TPRC 2019, July 2019, https://doi.org/10.2139/ssrn.3426222.
18. Ibid.
19. Man-In-The-Middle (MITM) is a kind of attack in which a malicious third party takes control of a communication channel. The attacker can intercept, modify, change, or replace target victims' communication traffic.
20. Mauro Conti, Nikola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," I*EEE Communications Surveys & Tutorials* 18, no. 3, March 2016, https://doi.org/10.1109/COMST.2016.2548426.
21. Side Channel Attacks pose a real and serious threat to user privacy as they present a way to defeat encryption using information leaking in a side-channel. Source: Chen, Shuo, Rui Wang, XiaoFeng Wang, and Kehuan Zhang, "*Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow,*" Proceedings of the IEEE Symposium on Security and Privacy (Oakland), May 2010, https://www.microsoft.com/en-us/research/publication/side-channel-leaks-in-web-applications-a-reality-today-a-challenge-tomorrow/.

NOTES

22. Eyal Ronen, Robert Gillham, Daniel Genkin, Adi Shamir, David Wong, and Yuval Yarom, "The 9 Lives of Bleichenbachers CAT: New Cache Attacks on TLS Implementations," 2019 IEEE Symposium on Security and Privacy (SP), 2019, https://doi.org/10.1109/sp.2019.00062.
23. Olav Lysne, Ahmed Elmokashfi, Niels Nagelhus Schia, Lars Gjesvik, and Karsten Friis, "Critical Communication Infrastructures and Huawei," TPRC 2019, July 2019, https://doi.org/10.2139/ssrn.3426222.
24. Ibid.
25. Ibid.
26. Ibid.
27. T. Buckman, "NATO Network Enabled Capability Feasibility Study," NATO Consultation, Command and Control Agency, October 2005, http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf.
28. Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare Blog, Lawfare Institute, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.