Build-A-Cyber-Attacker: Simulating Attackers to Reflect Myth and Folklore in Cyber Threat Analysis

Tim Pappa
Capitol Technology University, Laurel, Maryland, USA

tpappa@captechu.edu

Abstract: This practitioner's working paper explores the application of simulation exercises in cyber threat analysis, finding that the creative integration of conceptual frameworks like folklore and myth in practical instructional assignments and discussions can familiarize students with the influence of myth and folklore in their analysis. Simulation in this context is concentrated on the process of thinking through a series of events in an exercise, rather than focusing on the outcome. Prior research on simulation found that students were more likely to complete assignments on time and finish course projects with higher grades when they imagined when and how they would study. This practitioner's paper will present a working sample of simulation exercises, including a simulation exercise where graduate intelligence and military students were asked throughout the course to simulate and create the mythos of their own cyber threat attacker group, including their attacker group target portfolio and an outline of how they might respond to threats. These working exercises suggestively demonstrated the complexities of simulating the cultural and operational challenges of cyber threat attacker groups. These students had creative freedom to simulate these cyber threat encounters, even without foundational background or expertise in the countries or cultures they simulate. This exploratory practitioner's working paper suggests simulation can introduce further dimensionality to cyber threat intelligence analysis.

Keywords: Folklore; Myth; Simulation; Cyber Threat Analysis; Cyber Attacker

1. Introduction

This practitioner's working paper demonstrates how conceptual frameworks like folklore and myth can be applied, in a simulation project throughout a course where students create a fictional cyber attack group.

The author structured his original course curriculum with several assignments and discussions related to folklore and myth because of his background in law enforcement and intelligence, where he experienced firsthand what he believed was the influence of folklore and myth in mischaracterizations of cyberterrorism threats (Pappa, 2024). While there has been growing criticism of what at times has appeared to be commodification of characterizing the threat posed by cyber attackers, there has been limited commentary on the influence of folklore and myth on American cyber threat analysts and practitioners who characterize these cyber threats. This paper introduces a potential model for familiarizing students with the influence of folklore and myth, based on students' work in a graduate comparative cyber security course provided asynchronously online. Although the university where students enrolled in this paper is a private university, most of the students in this course are affiliated with the American military or American intelligence community.

Students in this course are immediately introduced to concepts of folklore and myth. To start preparing students for this simulation of creating a fictional cyber attack group, students were asked in the first week to write about their personal experience with cyber threats and what they believe is the biggest danger they face online. The assignment explored students' core beliefs about cyber threats, but additionally and more importantly, the assignment encouraged students to start thinking about why they believe a cyber threat is a danger to them or not. Students generally wrote about fraud and online crime, rather than nation state attackers, which governments and cybersecurity firms tend to warn people the most about.

The author also included additional assignments and reading in this graduate course related to folklore and myth in the initial weeks of the course. As another example, students were asked to select at least one example of a historical cyber threat event or attack and discuss how that event or attack reflected both myth and folklore. This asynchronous graduate course provided considerable reading samples to introduce and familiarize students with these frameworks. Some of those historical events included the *Syrian Electronic Army* and the *Islamic State Hacking Division*, for example. In both cases, these attack collectives were in fact one person or a limited collective in terms of people and threat or capabilities, but significant attention and resources were directed to countering these embellished cyber threats in their time. The assignment also asked students to "characterize the myth and folklore of US government cyber threats". Beyond the reading provided for students, the assignment instructions were limited to allow students to share freer commentary from their own perspective on myth and folklore. This kind of assignment with limited instructions was meant to encourage the students to consider alternative perspectives, such as the folklore and myth of the American government as an enterprise

with cyber attack groups. This assignment may have been most surprising to students, who were asked generally to write about the "real and imagined impressions we form of cyber threats", including if those threats come from their own government.

This practitioner's working paper will introduce some of the related work on the communication of folklore and myth. This paper will then describe additional background on this practice of simulation as an instructional method and how the author structured this assignment throughout the duration of the course. The author will share how two students in this course created fictional cyber attack groups, including samples from their written assignments demonstrating how they applied folklore and myth to the origin story of their fictional cyber attack group and how their fictional cyber attack group responded to false claims of attacks, for example. How a cyber attack group grows or maintains its reputation can be critical to its folklore or myth. This paper will conclude with a discussion of research limitations and future research.

2. Related Work: the "Branding" of Cyber Threats When Communicating Folklore and Myth

Gros (2021) in his longitudinal study of attacker behaviours may have definitionally conflated "myths and misconceptions", but his paper highlighted a fair criticism of cyber threat intelligence practitioners – that we do not necessarily know what kind of attacker we might face, so we generally approximate and sometimes overestimate attackers as "mythical, all-powerful creatures who can do whatever they want…they are treated as an undefined entity that represents every possible type of attacker".

Vigano (2024) encouraged the use of fairy tales and myths to explain cybersecurity or information security more generally to less technical or broader public audiences. Talbot, Frincke, and Bishop (2010) wrote about "demythifying cybersecurity", focusing instead on the common practices derived from so-called beliefs or sayings among practitioners in information security communities, such as "effective security is burdensome security". The author agrees that these perspectives are common in cybersecurity or information security, but the use of myth may be more likened to folklore or how people in those communities talk about it and how they learn about information security from talking about it with people they know in those communities.

The author suggests that this treatment of myth and folklore is a bit trivial, as referring to myth or folklore as an explanation of why people believe some things about cybersecurity, for example, can be useful, but this paper is exploring how folklore and myth as defined in more granular commentaries of that influence in cultures and groups can also influence or even bias our cyber threat analysis. There is some growing recognition of how the "branding" of generally unknown attackers as fearsome and dangerous can be misleading or inaccurate. Shires (2020) wrote that cybersecurity experts continually define or redefine characterizations of attackers. Shires referred to an example of the "Shadow Brokers" who were known for their alleged leak of American intelligence hacking tools and their alleged association with Moscow. Referring to Kumar (2017), Shires wrote that while the Shadow Brokers themselves did not suggest or encourage any prompts for how they should be visualized, "cyber-noir" imagery still emerged, with content such as "dark silhouetted figures in overcoats and fedoras against a red background".

Shires suggested that the "sophisticated cartoon style of graphic novels" and films like *Sin City* have perhaps influenced animations and illustrative representations of dangerous attackers. Shires referred to "Fancy Bear", the codename for a Russian attacker or attack group named by cybersecurity firm Crowdstrike. Fancy Bear appears to have glowing red eyes and a Soviet-style fur hat, he wrote. Shires introduced the term "cyber-noir" when talking about the "branding" he has observed in the cybersecurity industry:

Many emerging companies in the cybersecurity industry deliberately play on the popular perception of cybersecurity as a nether region, a gloomy underworld in which the good guys must resort to unconventional tactics to keep at bay a motley group of threats to the digital safety of unsuspecting individuals, businesses, and governments…These choices are part threat construction, part branding, and part knowing in-jokes, and they are selected just as often by the analysts themselves as they are chosen by marketing departments.

This paper suggests that concepts of folklore or the communication of folklore and even myth may also explain this kind of demonstrated influence or even manipulation of how attackers are characterized as threatening. Ben-Amos (2014) modelled efforts by young anthropologists in the early 1970s who began to grow the definition of folklore, beyond just "orality" or more traditional storytelling. Ben-Amos began characterizing folklore generally as something that is understood only when associated with a structured group of some kind and within a social context of some sort. "Folklore" is first understood in its relationship to and possession by a group of

people. This is just an abstraction for the purpose of using a methodology to examine the phenomena. Examining phenomena as folklore in its cultural context involves observing and characterizing a "communicative process" rather than just identifying an "aggregate of things".

If the cultural mode of communication is the key for definition, he wrote, then all these forms are but different phases within the observed characteristics of a group. Folklore is therefore communication of something that takes place between people. When viewed as a process, folklore can be considered as a form of interaction rather than just a marginal projection or reflection of other social phenomena. This has been called "living folklore" or even "growing folklore" by Soviet folklorists, observing an "ever-growing, changing, living thing". This appears to suggest Shires' characterization of the cybersecurity industry demonstrates this communication of folklore among people with shared interests. Ben-Amos (1971) proposed that folklore was "artistic communication in small groups" *in context*. Meaning again that if we are trying to understand the folklore we are observing, we cannot separate what is being communicated and why from the group of people communicating.

Much of the research literature exploring the difference between folklore and myth has generally characterized myth as something much more sacred. Blout (2017, 2023) has written extensively about the *myth of foreign conspiracy*, examining the narratives of Iranian leaders who propagate attempts by the West to undermine Iran. Many historians have defined myth from a similar perspective – that people can point to actual historical events but then *naturalize* those events and a new myth story with emotion. Suggesting to Iranian audiences a myth of foreign conspiracy such as 'the West wants to overthrow us' is part of a "myth-story" because of events like the 1950s coup attempt in Tehran. This "historical capital" can be represented in state narratives and personal worldviews. Kaser and Halpern (1998) wrote that we could also call this "symbolic capital" because this kind of myth making happens within particularized cultural frameworks. The perception of "sacredness" in a myth unlike some definitions of folklore is often found in narratives associated with the historic fate of a people or a nation. Kaser and Halpern emphasized that these repeated myths never exist in a neutral space, but rather national myths are defined in reference to others. The author suggests these "repeated myths" and communication of folklore happen in offensive and defensive spaces, such as operational squads and analytical units. He has experienced this communication firsthand. These are often "national myths" as well, when considering the branded threats of nation state attackers and cybercriminal attackers who have been or appear to be attacking American critical infrastructure and organizations.

3. Method: Simulation as an Instructional Strategy and a Process of Decision Making

Much of the research literature on cybersecurity education and training has increasingly explored the use of simulation, but primarily from the perspective of simulated cyber ranges and simulated network attack and defence scenarios (Tymoshchuk et al., 2024; Alnajim et al., 2023; Katsantonis et al., 2023; Chowdhury, Katsikas, and Gkioulos, 2021). This paper focuses on simulation as a method for guiding how students think through the creation of their fictional cyber attack group.

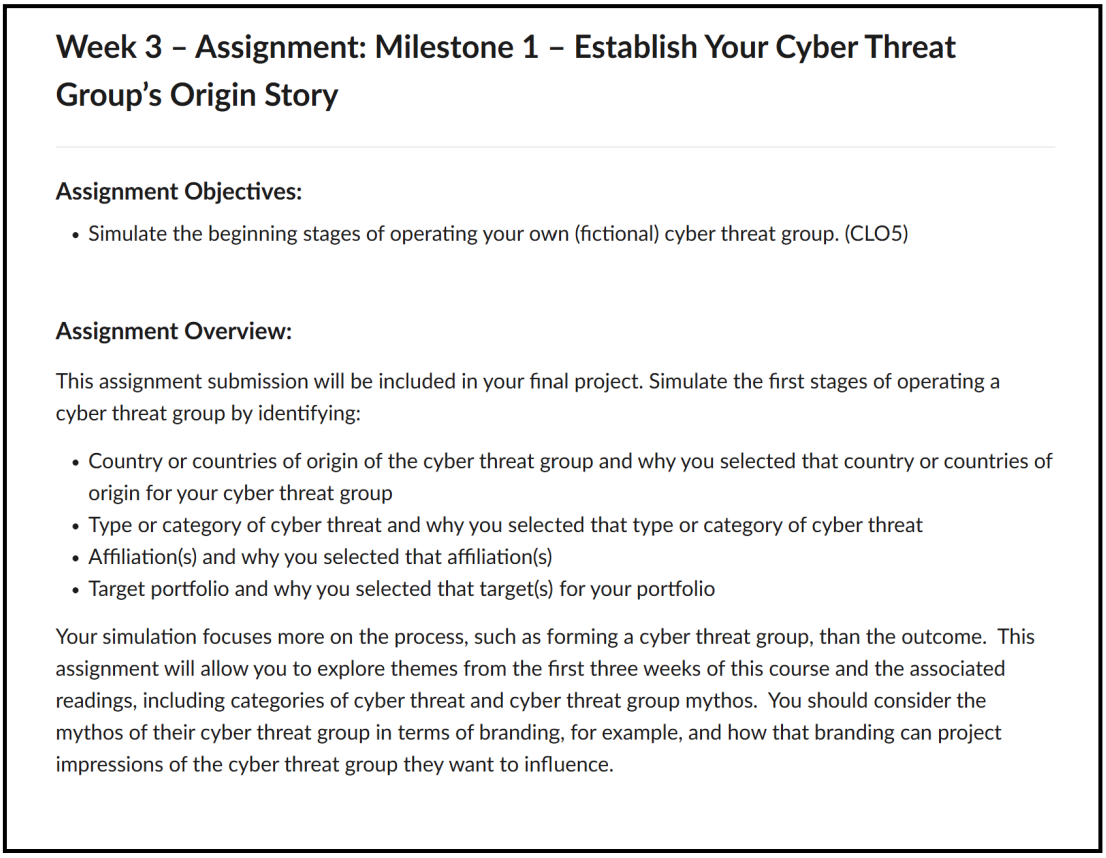
Taylor and Schneider (1989) defined simulation as a "cognitive construction of hypothetical scenarios", where someone thinks through or imagines usually in sequential stages or steps what they might do in a hypothetical or anticipated situation. People tend to think about anticipated events, like a rehearsal of what they think will happen and what they think they will do. Taylor and Schneider noted that simulation can be key for problem solving. Taylor and Schneider referred to Kahneman and Tversky's (1982) description of the heuristic simulation, where someone's availability bias can influence what they determine might be a solution or an approach to an anticipated event or interaction. Kahneman and Tversky characterized the simulation heuristic as a "shortcut" for making predictions or estimating probabilities or assessing causality. Simulations are not necessarily scripts, they wrote. A script is a schema that describes an expected sequence of events in a familiar situation, such as going to a movie or making coffee. Taylor and Schneider, however, wrote that a simulation could be characterized as a "dynamic representation" of a script, although not all simulations require a script. Simulation is a method of planning, rather than focusing on the outcome as most people do.

Unlike many instructional methods, simulation generally concentrates on how people function in a social environment (Jones and Barrett, 2017; Ouahi et al., 2021). Simulation can be adapted to a students' cognitive needs and abilities. Taylor et al. (1998) referred to a study that asked participating students to simulate the steps they would take to study for a future exam, finding that the students focused on the planning phases during their simulation exercises did somewhat better on the exam than students who focused on the outcome. Taylor et al. wrote about the planning fallacy, where people tend to underestimate the resources needed for projects

and overestimate how easily it can be done. Taylor et al. found in a similar study that participating students who simulated the number of hours needed to study for an exam also scored better on an exam than students who simulated the outcome only.

Scherb et al. (2023) resembled some of the approach of this paper, recognizing that users must experience some of the perspective of an attacker to better understand how an attacker might target their organization. Scherb et al. created a rudimentary cyberattack simulation or "serious game" that asked students to demonstrate the role of an attacker crafting phishing and spear phishing emails as if they were attacking their own organization. Students had to essentially simulate the process of researching an organization, finding what they believed might be vulnerabilities, and then crafting an email that may influence a target user to click on a link or respond behaviorally as the attacker intended. The researchers wanted this game or simulation to be as realistic as possible, so students were also required to find fake websites for phishing attacks and simulate the purchase of exploits on a fictional darknet market. In this simulation study, they found that there was marginal improvement in students' ability to understand and detect phishing or spear phishing attempts, in contrast to other user training methods that have generally been viewed as less effective.

The author organized this project so that students would complete assignments developing their fictional cyber attack group three times throughout the course, including in a final assignment where students were presented with several scenarios in which they had to visualize how their cyber attack group would respond. Students read the following objectives and overview for each phase of the assignment:



Week 3 – Assignment: Milestone 1 – Establish Your Cyber Threat Group's Origin Story

Assignment Objectives:

- Simulate the beginning stages of operating your own (fictional) cyber threat group. (CLO5)

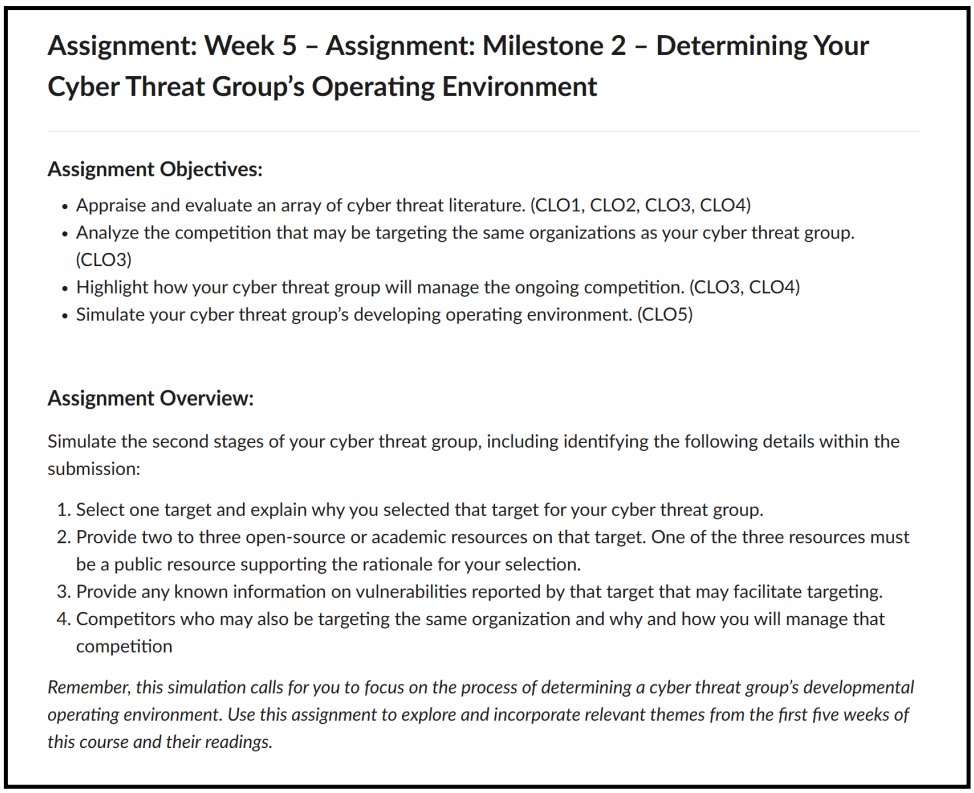
Assignment Overview:

This assignment submission will be included in your final project. Simulate the first stages of operating a cyber threat group by identifying:

- Country or countries of origin of the cyber threat group and why you selected that country or countries of origin for your cyber threat group
- Type or category of cyber threat and why you selected that type or category of cyber threat
- Affiliation(s) and why you selected that affiliation(s)
- Target portfolio and why you selected that target(s) for your portfolio

Your simulation focuses more on the process, such as forming a cyber threat group, than the outcome. This assignment will allow you to explore themes from the first three weeks of this course and the associated readings, including categories of cyber threat and cyber threat group mythos. You should consider the mythos of their cyber threat group in terms of branding, for example, and how that branding can project impressions of the cyber threat group they want to influence.

Figure 1: In week 3 of this course, the author assigned the first step in the students' project creating their own cyber attack group – establishing an origin story. The first two weeks of asynchronous online instruction included reading and writing assignments related to assessing their own impressions of cyber threat and how folklore and myth may have shaped perceptions of historical cyber attacks and cyber attack groups. The assignment overview provided some instruction on completing the first stages of creating a cyber threat group and additional background on simulation.



Assignment: Week 5 – Assignment: Milestone 2 – Determining Your Cyber Threat Group's Operating Environment

Assignment Objectives:

- Appraise and evaluate an array of cyber threat literature. (CLO1, CLO2, CLO3, CLO4)
- Analyze the competition that may be targeting the same organizations as your cyber threat group. (CLO3)
- Highlight how your cyber threat group will manage the ongoing competition. (CLO3, CLO4)
- Simulate your cyber threat group's developing operating environment. (CLO5)

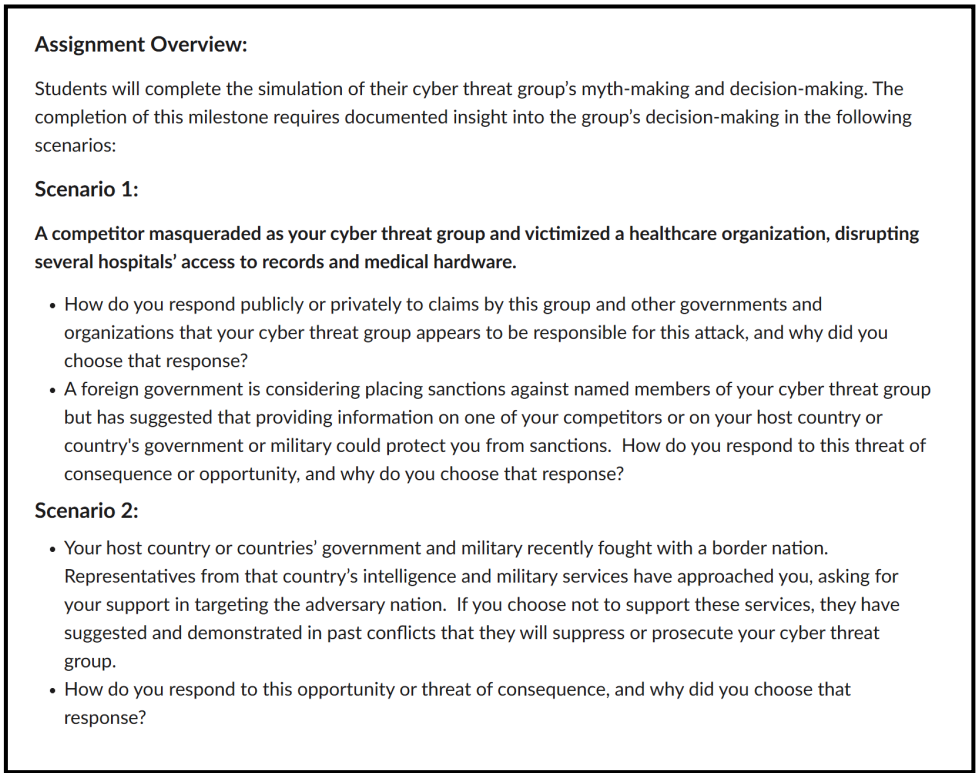
Assignment Overview:

Simulate the second stages of your cyber threat group, including identifying the following details within the submission:

1. Select one target and explain why you selected that target for your cyber threat group.
2. Provide two to three open-source or academic resources on that target. One of the three resources must be a public resource supporting the rationale for your selection.
3. Provide any known information on vulnerabilities reported by that target that may facilitate targeting.
4. Competitors who may also be targeting the same organization and why and how you will manage that competition

Remember, this simulation calls for you to focus on the process of determining a cyber threat group's developmental operating environment. Use this assignment to explore and incorporate relevant themes from the first five weeks of this course and their readings.

Figure 2: In week 5, the author asked students to continue developing their fictional cyber attack group. Students were asked to start creating a target portfolio for their cyber attack group and to provide analysis on the selection of those targets. This exercise was designed to help students think through the challenges and opportunities based on their cyber attack group's chosen operating environment.



Assignment Overview:

Students will complete the simulation of their cyber threat group's myth-making and decision-making. The completion of this milestone requires documented insight into the group's decision-making in the following scenarios:

Scenario 1:

A competitor masqueraded as your cyber threat group and victimized a healthcare organization, disrupting several hospitals' access to records and medical hardware.

- How do you respond publicly or privately to claims by this group and other governments and organizations that your cyber threat group appears to be responsible for this attack, and why did you choose that response?
- A foreign government is considering placing sanctions against named members of your cyber threat group but has suggested that providing information on one of your competitors or on your host country or country's government or military could protect you from sanctions. How do you respond to this threat of consequence or opportunity, and why do you choose that response?

Scenario 2:

- Your host country or countries' government and military recently fought with a border nation. Representatives from that country's intelligence and military services have approached you, asking for your support in targeting the adversary nation. If you choose not to support these services, they have suggested and demonstrated in past conflicts that they will suppress or prosecute your cyber threat group.
- How do you respond to this opportunity or threat of consequence, and why did you choose that response?

Figure 3: In week 8, the final week of the course, students were asked to complete the creation of their fictional cyber attack group by responding to various scenarios that should challenge their cyber attack group's decision making and "mythos".

The following section features samples from two students who completed this simulation.

4. A Simulation of Students' Fictional Cyber Attack Groups

4.1 Establishing Your Cyber Attack Group Origin Story and Target Portfolio

Student 1 named his fictional cyber attack group the "Nguyen Van Ly Alliance" (NVLA), basing his group in Vietnam. He characterized his group as a hacktivist group that formed in response to the growing political dissent online against the government's authoritarian practices. He wrote that the NVLA organized in opposition to the government to "disrupt government bodies from continuously harassing and arresting those who seek to vocalize their desire for a more free and accepting Vietnam".

Student 1 wrote that the NVLA will primarily utilize Distributed-Denial-of-Service (DDoS) attacks against the Vietnamese government, because of how accessible those tools or services are. The student referred to the "underground support" from other activists in Vietnam who oppose the government but want to remain largely private. When the NVLA can showcase local support, it gives the NVLA a "sense of legitimacy". The student also suggested the Vietnamese diaspora who do not support the government could also provide funding. Student 1 described the target portfolio of the NVLA, concentrating primarily on the Ministry of Public Security, because of that agency's state surveillance and censorship. Student 1 wrote that another target will include state-owned enterprises, such as the Vietnam Electricity (EVN) and Viettel Military Industry and Telecoms Group, because they appear to support the Ministry of Public Security in its efforts against Vietnamese communities advocating for human rights and free speech.

Student 1 referred to a real figure when discussing the "mythos" of the NVLA. He wrote that Thadeus Nguyen Van Ly was a Catholic Vietnamese priest who was imprisoned for more than 15 years because of his pro-democracy activism related to human rights. Student 1 wrote that his cyber attack group is named after Van Ly because Vietnamese people who are familiar with Van Ly's human rights activism "will be inspired by the name and actions of the group" in his name. He wrote that the Vietnamese government may also be troubled by a hacktivist group claiming to represent the name and movement of a human rights activist in Vietnam that has challenged the government.

Student 2 characterized his cyber attack group as a Russia-based group focused on ransomware and cyber espionage, operating mostly with cybercriminal gangs and some indirect Russian government support. Student 2 wrote that because of the "safe operational environment" in Russia, his group has more opportunity to recruit talented attackers and to be "ambitious" if his group's objectives appear to align with Moscow. Student 2 appeared to be much more instrumental in explaining his choice of affiliations and group origin; he emphasized more than once that his group is not directly supporting Moscow, but his group needs the safety of operating in Russia to accomplish its goals. He wrote that his group's targets would include critical infrastructure sectors, including healthcare and energy as well as technology and defence firms in Europe and in the United States. He wrote that this approach would "satisfy" his group's financial and strategic motivations. Student 2 explained that healthcare organizations are typically more vulnerable and more willing to pay ransoms to restore their access, and that data stolen from technology and defence firms is more valuable for resale or sharing, including to the Russian government. He wrote that this "careful planning and strategic alignment" would be essential for his cyber operations to be successful.

4.2 Managing Your Operational Environment and Competitors

Student 1 suggested that if the NVLA consistently targeted Vietnamese state telecommunications firms affiliated with security services, the result could be a reduction in customer satisfaction and a reduction in these state firms' revenue. One of these firms also develops weapons systems, so there is the possibility NVLA could disrupt revenue streams to those weapons projects. There is symbolic value in targeting these firms because of their surveillance in support of the government, but also because the government may suffer reputational damage as well if these attacks are publicized.

Student 1 wrote that his two main competitors would likely be China-sponsored cybercriminal collectives or groups and ransomware gangs. He suggested that because China has demonstrated interest in targeting government telecommunications organizations to collect data and enhance their surveillance of that target country and region, China may be targeting the same telecommunications firms in Vietnam. Student 1 suggested his group would avoid "clashing" in any cyber attacks with a China-affiliated cyber attack group but could instead

"piggyback" off any known attack to expose vulnerabilities further. Student 1 recognized that although observers could conclude that NVLA's threat activity was also the same China-affiliated attackers and there would be less suspicion of NVLA by Vietnamese authorities, the public may also assume China was responsible. That affiliation "would impact [NVLA's] mythos in that the public and their target would not effectively receive the NVLA's message of freedom for the Vietnamese public".

Student 2 wrote that he anticipated several rivals when targeting western Europe's energy infrastructure. He wrote that "maintaining flexible operational strategies" could help minimize detection and conflict with competing attackers, including by coordinating with Moscow to gain advantage. While student 2 did not write as much about the folklore or myth of his fictional cyber attack group, he did appear to recognize the folklore and myth of Russian targeting of western European infrastructure and how those disruptions can "create political pressure, influence policy decisions, or sow discord" among allied countries in that region. Student 2 wrote that if his attack group could cause these kinds of disruptions, "they could effectively weaken the collective resilience" of those allied countries and build support for his group from Moscow.

4.3 Cyber Attack Group Decision Making in Various Scenarios

The first scenario for the final phase of Student 1's simulated cyber attack group involved an unknown competitor masquerading as the NVLA while victimizing a Vietnamese healthcare organization. Student 1 wrote that the NVLA would publicly deny responsibility for the attack, noting that targeting a Vietnamese healthcare organization contradicts the NVLA mission. The first scenario also stated that a foreign government suggested it was considering placing sanctions on the NVLA unless the NVLA provided evidence they were not involved in the attack or that someone else was responsible. Student 1 wrote that agreeing to find evidence would provide an "opportunity for ideological progress to gain international awareness and support", much like Anonymous in the past has improved the collective's reputation after assisting in campaigns against dark web sites hosting explicit content, such as images of child sexual abuse. The second scenario involved a recent border conflict between Vietnam and another country. Vietnamese intelligence and military services approached NVLA representatives asking for cyber attack support against the other country involved in the border conflict. Vietnamese services told NVLA they will prosecute or suppress NVLA if the NVLA does not assist them. Student 1 wrote that the NVLA would provide "limited and indirect assistance" because part of their mission includes protecting the freedoms of the Vietnamese people, which would perhaps be disrupted or restricted if a war resulted from this border conflict. The NVLA would attempt to limit any direct cooperation with the Vietnamese government to "retain their ideological integrity to balance their operational goals with public perception within Vietnam".

Student 2 framed the response of his fictional cyber attack group to similar allegations related to an attack on a healthcare organization by detailing a public response and a private response. He wrote that his group would deny involvement and then voluntarily provide material evidence such as time-stamped logs and other operational records that appeared to demonstrate the group was inactive during the timing of the alleged attack. His group would also offer publicly to collaborate with law enforcement. Student 2 wrote that if he could identify the attack group masquerading as his cyber attack group, there may be options for retaliation, such as materially revealing their involvement or exposing their operational infrastructure. He suggested that this approach could discourage future groups from masquerading as them in an attack. Student 2 wrote that in the second scenario, cooperation with Russia would be the only option and that cooperation may strengthen his group's position within Russia's "cyber and geopolitical ecosystem, opening opportunities for resources, intelligence, and operational support". Ultimately, he wrote, the most immediate concern in this scenario is "ensuring the survival of the cyber threat group". Student 2 referenced the enhanced access to tools and information sharing that could result from that support, but much of this decision appeared to benefit the folklore and myth of Russia's attack capabilities and targeting interests and objectives in western Europe, more so than the student's cyber attack group.

5. Limitations and Discussion

The sample of simulated cyber attack groups derived from this graduate course is small. As such, the author considers this working paper to be exploratory because of that limited sample size.

The author could have provided additional instruction in this series of assignments throughout the course, to provide additional commentary on the folklore and myth of their cyber attack group. The author chose not to, so that these students would naturally simulate their fictional cyber attack group.

Student 1 wrote in his conclusion in the final phase of his project that the need for NVLA to blend "ideological purpose with adaptive tactics to persevere" is important especially as global cyber conflicts grow more complicated. Student 2 also appeared to suggest in several of his assignments that there were instrumental motivations for supporting Moscow and targeting similar infrastructure to preserve and grow his attack group. The author would argue these nuanced motivations are rare when compared to much of the commentary on motivations of cybercriminals and cyber attackers who appear to be aligned with nation state enterprises. When there is limited insight into the attribution or affiliation of cyber attackers or cyber attack groups that appear to resemble or be aligned with the interests of a nation state attack enterprise, there often appears to be suggestions of collusion with or support to that nation state enterprise. While that is sometimes the case, both students found that their own cyber attack group objectives only appeared to align with or support the government whenever there was some coercion or some anticipated loss if they did not support them. These kinds of nuances in cyber threat intelligence can significantly impact the analysis of threat and motivation.

Ethics Declaration

Ethics clearance was not required for this research. The author did obtain written permission from both students to sample some of their work in this paper.

AI Declaration

AI tools were not used in the creation of this paper.

References

Alnajim, A.M., Habib, S., Islam, M., AlRawashdeh, H.S. and Wasim, M., 2023. Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, *15*(12), p.2175.

Ben-Amos, D., 1971. Toward a definition of folklore in context. *The Journal of American Folklore*, *84*(331), pp.3-15.

Ben-Amos, D., 2014. A definition of folklore: A personal narrative. *Estudis de Literatura Oral Popular/Studies in Oral Folk Literature*, (3), pp.9-28.

Ben Ouahi, M., Lamri, D., Hassouni, T. and Al Ibrahmi, E.M., 2022. Science Teachers' Views on the Use and Effectiveness of Interactive Simulations in Science Teaching and Learning. *International journal of instruction*, *15*(1), pp.277-292.

Blout, E.L., 2017. Soft war: Myth, nationalism, and media in Iran. *The Communication Review*, *20*(3), pp.212-224.

Blout, E.L., 2023. Media and Power in Modern Iran.

Chowdhury, N., Katsikas, S. and Gkioulos, V., 2022. Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*, p.102551.

Groš, S., 2021. Myths and misconceptions about attackers and attacks. *arXiv preprint arXiv:2106.05702*.

Jones, J.D. and Barrett, C.E., 2017. Simulation as a Classroom Teaching Method. *Journal on School Educational Technology*, *12*(4), pp.49-53.

Kaser, K. and Halpern, J.M., 1998. Historical myth and the invention of political folklore in contemporary Serbia. *Anthropology of East Europe Review*, *16*(1), pp.89-107.

Katsantonis, M.N., Manikas, A., Mavridis, I. and Gritzalis, D., 2023. Cyber range design framework for cyber security education and training. *International Journal of Information Security*, *22*(4), pp.1005-1027.

Scherb, C., Heitz, L.B., Grimberg, F., Grieder, H. and Maurer, M., 2023. A cyber attack simulation for teaching cybersecurity. *EPiC Series in Computing*, *93*, pp.129-140.

Shires, J., 2020. Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, *41*(1), pp.82-107.

Smith, M.W., 1959. The importance of folklore studies to anthropology. *Folklore*, *70*(1), pp.300-312.

Talbot, E.B., Frincke, D. and Bishop, M., 2010. Demythifying cybersecurity. *IEEE Security & Privacy*, *8*(3), pp.56-59.

Taylor, S.E. and Schneider, S.K., 1989. Coping and the simulation of events. *Social cognition*, *7*(2), pp.174-194.

Tymoshchuk, D., Yatskiv, V., Tymoshchuk, V. and Yatskiv, N., 2024. Interactive cybersecurity training system based on simulation environments. *arXiv preprint arXiv:2501.00186*.

Viganò, L., 2024. The cybersecurity of fairy tales. *Journal of Cybersecurity*, *10*(1), p.tyae005.