Human Factors in Cybersecurity, Vol. 91, 2023, 20–27
https://doi.org/10.54941/ahfe1003716

Out of Sight but Still in Mind: Making 'Invisible' Cyber Threats More Salient via Concrete Analogies

Aryn Pyke[1,2], Rebecca Bouchelle[2], and David Uzhca[2]

[1]Army Cyber Institute, West Point, NY 10928, USA
[2]United States Military Academy, West Point, NY 10996, USA

ABSTRACT

It can be easier to conceive of and anticipate physical threats than cyber threats. Cyber threats can involve unseen remote hackers and can capitalize on invisible wireless signals as vectors. As such cyber threats are often out of sight and out of mind. How can we make these abstract, 'invisible' threats more intuitive and salient? We employed concrete analogies to enable future Army Officers to better anticipate cyber threats in tactical contexts. Modern multi-domain battle involves not only physical threats like fire fights and improvised explosive devices (IEDs), but also, increasingly, cyber threats. For example, the enemy may jam, intercept or track communication signals, hack into computing systems to exfiltrate or alter information, and/or hack equipment with electronic and autonomous components (including navigation systems, drones and robots). To ensure readiness, all soldiers, (not only cyber specialists) must have some awareness of this 'threatscape'. We developed the problem anticipation task (PAT) to gauge the degree to which participants would anticipate cyber as well as non-cyber tactical threats. They read a hypothetical mission description and tried to anticipate various problems that could arise. The mission explicitly mentioned several cyber-vulnerable components (e.g., radios, navigation systems, drones, biosensors, cell phones). Prior research using a sample from the same population indicated that about 40% of subjects did not anticipate a single cyber threat (Pyke, Ness & Feltner, 2023). The current research used the PAT as a pre- and post-test and included an intervening intervention. Experimental subjects read a passage about a fictitious historical mission set in the 1800s. The version of the passage presented to the experimental group included historical issues (e.g., carrier pigeon intercepted by enemy) that were intended to be analogous to modern cyber-related issues (e.g., wireless communications signal intercepted/tapped by enemy). The intervention for the comparison group involved a passage describing historical issues (e.g., horse losing a shoe) that were intended to be analogous to modern non-cyber related issues (e.g., vehicle breakdown). Note that the link to the corresponding modern situation was not made explicit to the participants, they were just exposed to a historical situation that could lend itself to being analogous to a modern cyber situation. For the experimental group (but not the control) there was a significant gain in the percent of participants who were able anticipate one or more cyber issues. Thus, concrete analogies can serve to make 'invisible' cyber threats more intuitive and easier to anticipate.

Keywords: Cybersecurity, Cyber analogies, Anticipating cyber threats, Problem anticipation task (PAT)

INTRODUCTION

It is often important for us to be aware of things – especially potential threats – that may not be naturally salient or perceptible via our senses. Tools like microscopes, night vision goggles and augmented reality goggles can augment our sensory perception and allow typically 'invisible' entities to become visible. Rendering something no longer 'out of sight' is one way, but not the only way, to help an individual keep that something in mind. To help our participants to keep unseen things (here, cyber threats) in mind, rather than making them ***visible***, our approach was an intervention to make them easier and more intuitive to mentally ***visualize***.

One way to help individuals visualize and better understand unseen entities, like germs, is to expose them to representations generated by illustrators and graphic designers that can make certain properties such as contagion risk and mobility more salient (Stone, Stark & Rutter, 2022). Another approach, which is the approach we used, is via analogies. Before discussing further details of our approach, we will first briefly describe the 'use case' for our participants and the results of a prior study to motivate the need for increased awareness of cyber threats.

Anticipating Cyber Threats in Tactical Contexts

In modern multi-domain warfare, cyber is one of the five key domains, and engagements may increasingly involve cyber elements (Schneier & Wheeler, 2021). Thus, in addition to posing physical threats like firefights and improvised explosive devices (IEDs), the enemy may also jam, intercept or track communication signals, hack into computing systems to exfiltrate or alter information, and/or hack equipment with electronic and autonomous components (including navigation systems, drones and robots). To ensure readiness in a multi-domain context, all military personnel must develop a mindset that includes an awareness of the modern threatscape, and that allows them to anticipate possible cyber as well as non-cyber threats. The need for increased cyber awareness among all military personnel was highlighted by the news that military base locations were being revealed due to the upload of soldiers' jogging routes recorded by their personal fitness-tracking devices (Hsu, 2018).

As such, it has been suggested that Army educational/training programs should prepare all soldiers for the exigencies of cyberwarfare (Heatherly & Melendez, 2019). This need raised two research questions: i) how can we assess soldiers' level of awareness of cyber vulnerabilities; and, if necessary, ii) how might we further improve it? The first question, about assessing baseline awareness, was addressed in prior research (Pyke, Ness & Feltner (2023)), so the current study was focused on point (ii) – developing a short, simple intervention to improve cyber awareness.

To assess baseline awareness of cyber threats, Pyke et al.(2023) developed a Problem Anticipation Task (PAT): Future Army Officers were asked to read a brief description of a hypothetical tactical mission, and then were asked to list up to 25 things that could go wrong on that mission. The researchers sought to determine the number and types of cyber-related issues that participants

might spontaneously list, if any (e.g., hacking equipment, data alteration or exfiltration, signal jamming, interception and/or tracking, etc.) relative to more traditional non-cyber issues that may arise (e.g., ambush, vehicle malfunction, running out of ammunition, etc.). To support the chances that participants might identify cyber issues, the mission descriptions made explicit mention of cyber-vulnerable components (radios, navigation systems, biosensors, satellites, drones, and cell phones). Although participants were digital natives, only 8% of anticipated problems were cyber related and the data revealed that 39% of participants did not list any possible cyber issues at all among the problems they anticipated. These results suggested that there was room for improvement in future Officers' awareness of cyber threats, which motivated our development of an intervention.

We intuited that one reason cyber threats are less likely to come to mind is that they may not make a direct or distinctive impact on our senses. For example, the wireless communications and data signals that support modern warfare, and which travel to and from radios, satellites, drones, cell towers, wifi hubs, biosensors, et cetera, are invisible. Thus, in contrast to physical threats like IEDs, cyber threats may be more difficult to mentally visualize and therefore more difficult to anticipate. In comparison to tangible targets (e.g., soldiers, convoys, and bases), which are vulnerable to kinetic attacks, the invisible communication signal and electronic data storage targets of cyber-attacks are, quite literally, out of sight, and often, therefore, out of mind.

Prior to the advent of modern wireless telecommunications, information exchange methods often afforded more salient concrete or visible cues (e.g., telegraph lines, carrier pigeons, and light signals etc.), so that one might more readily conceive of the possibility of enemy detection or disruption of such channels. Similarly, prior to the digital storage of documents and data in computing devices, paper documents could be physically stolen (exfiltrated), looked at, or physically altered/doctored. Such activities involving an in-person human interacting physically with material objects can be more easily pictured (and thus more easily anticipated) than an 'invisible'/remote hacker gaining access to a black-box computing system via means that are mysterious to most of us, and interacting with digital data that cannot be directly seen or touched. This reasoning led to our development of an intervention involving concrete physical analogies to make cyber threats more salient.

Affordances of Analogies

Analogies can support learning and problem solving by inviting a mapping between a familiar and/or concrete domain and an unfamiliar and/or abstract domain. Gick and Holyoak (1980) researched the use of analogy to guide problem solving using a pair of analogous problems. The unfamiliar and abstract problem was Dunker's (1945) radiation/tumor problem in which a patient has an abdominal tumor that can not be treated with medicine nor removed surgically but only destroyed by radiation. The problem is that the intensity of the ray required to kill the tumor would also inflict an unacceptable level of damage to the intervening healthy tissue on route. What

is the doctor to do? Note that to the subjects this problem was technical (like cyber) and involved the invisible (also like cyber).

Gick and Holyoak (1980) investigated whether subjects might have greater success in generating a possible solution to the Dunker problem if they were exposed to an analogous military problem. In this analogous problem, an army aims to attack a fortress ruled by a dictator, and if the full army arrives and attacks at once victory is assured. The general had his army gathered at the start of one of the many roads leading to the fortress, but just as he was about to advance he learned that the dictator had placed a mine on the road so that only small parties (not an Army) could traverse it without setting off the mine. The general also could not re-direct his Army to use another road to the fortress, because all roads had been similarly mined. The general nonetheless devised a way to fulfill the mission by dividing his army into small groups and dispatching each group to a take different road to the fortress, timed so that all the groups arrived at the fortress at once.

One could map this solution of the military problem to the Dunker problem as follows: Instead of sending a single strong ray of radiation through the body to the tumor, one could direct several lower power rays towards the tumor from different angles. These individual lower intensity rays will not prohibitively destroy the intervening healthy tissue, but when all these rays simultaneously meet at the tumor, together their net power will be sufficient to kill it.

THE PRESENT RESEARCH

In the present research, we developed, applied and assessed a short, simple analogy-based intervention intended to improve the awareness of and ability to anticipate potential cyber threats in a tactical context. To assess the effectiveness of our intervention, we used the Problem Anticipation Task (PAT; Pyke et al., 2023), as a pre and post-test.

Our intervening intervention required participants to read a passage containing analogies. The version of the passage presented to the experimental group included historical issues (e.g., carrier pigeon intercepted by enemy) that were intended to be analogous to modern cyber-related issues (e.g., wireless communications signal intercepted/tapped by enemy). The intervention for the comparison group involved a passage describing historical issues (e.g., horse losing a shoe) that were intended to be analogous to modern non-cyber related issues (e.g., vehicle breakdown). These hypothetical historical issues and the intended modern analogues are summarized in Table 1 (C1-C6 for the experimental group; N1-N6 for the comparison group). Note that participants were not privy to the intended modern analogies, rather the task encouraged them to draw analogies for themselves. Each passage contained six different historical issues.

We hypothesized that the experimental group, which was exposed to historical issues analogous to modern cyber-related issues (C1 – C6 in Table 1), would show a greater gain from pre- to post-test in two measures: i) the percent of participants to anticipate at least one cyber issue; and ii) the percent of anticipated issues that were cyber versus non-cyber.

Table 1. Hypothetical historical issues in the intervention and their intended modern analogues.

Historical Issue[a]	Intended Modern Analog[b]
C1. Messenger route blocked by enemy	Communication signal jammed
C2. Lost access to [paper] maps due to enemy	GPS hacked or jammed by enemy
C3. Hot air reconnaissance balloon disabled by enemy	Drone shot down (or Satellite communication disabled)
C4. Mirror communication signals using light (almost) tracked by enemy to our position	Enemy uses wireless signal (e.g., cell phone) to find/track your position
C5. Message transmitted by air (carrier pigeon) intercepted and/or enemy returned fake reply	Wireless signal interception & alteration
C6. Enemy infected horse feed with virus that made horses behave unpredictably and difficult to control	Enemy hacks equipment and installs virus that interferes with functioning/behavior of equipment.
N1. Ran out of food for horses	Vehicle runs out of gas (or general supply shortage)
N2. Horse lost a shoe	Vehicle gets a flat tire or breaks down
N3. Sprained wrist in fall, and suffering from dysentery	Medical issue(s) not caused by enemy
N4. Had a turn-coat in our midst who leaked intel to the enemy	Traitor/intel leak
N5. Fog caused visibility/navigation issues (Jeremiah & Billy Jr. got lost)	Visibility/navigation issues, not caused by enemy
N6. Enemy had blocked our route	Enemy had blocked our route.

[a] The historical issues were presented within a passage, structured as a letter from a soldier to his mother, about issues that arose on a fictitious historical mission (circa 1850). Issues C1–C6 were in the experimental group's version of the passage, and issues N1-N6 were in the comparison group's version of the passage.
[b] Subjects did not see the intended modern analogues in the second column.

METHODS

Participants

Cadets at the United States Military Academy (N = 93; mean age: 20.1 years, SD = 1.5) received course credit for participating. These individuals are slated to become future Officers in the United States Army. In terms of college level, there were 12 seniors, 33 juniors, 8 sophomores, and 39 freshman who participated (and 1 missing cell). In terms of college major, 30% were Social Science/Humanities majors and 70% were STEM (Science, Technology, Engineering and Math) majors. Information about sex assigned at birth was only collected for about half the subjects (N = 48) and of these 35% were female. Then, at the request of the Institutional Review Board during study renewal, this question was removed as it was not a factor in our hypotheses.

Procedure

Participants used their own computers to participate online via a web link. The experiment was implemented using the Qualtrics platform. Stimuli and

questions were presented on the screen as black text on a white background. The study had three parts: a pre-test, an intervention, and a post-test. The pre- and post-test each consisted of a PAT. A random number generator was used to randomly assign participants to a condition. The intervention for the experimental group (N = 47) involved having participants read a passage describing historical issues that were intended to be analogous to modern cyber-related issues. The intervention for the control group (N = 46) involved a passage describing historical issues that were intended to be analogous to modern non-cyber related issues. The whole procedure took about 30 minutes.

Problem Anticipation Task (PAT): This task was initially developed and deployed by Pyke et al., (2023) to gauge baseline cyber threat awareness in a different sample from the same population. In the current study, this task was used as the pre- and post-test to assess the effectiveness of our intervention. The PAT instructions were as follows: "As a military leader it is important to be able to anticipate (and ultimately plan for) possible things that could go wrong on a mission. Next, you'll read a paragraph describing a hypothetical tactical mission. As you read it, try to consider various possible kinds of problems that might arise". Participants then read one of two possible brief descriptions of hypothetical mission scenarios, Mission X (311 words) or Mission Y (313 words). A random number generator was used to counterbalance the use of Mission X and Y across the pre- and post-test. The goal of Mission X was to travel to meet with a leader of a local friendly faction and the goal of Mission Y was to set up an observation post. Each mission explicitly mentioned several cyber-vulnerable components (e.g., radios, navigation systems, satellites, drones, biosensors, and cell phones). At the bottom of a mission participants were reminded to consider a variety of different problems that might occur, and that it was "OK" to suggest some creative possibilities that might not be very likely.

Participants in the current study were then asked to describe 15 possible problems that might arise. They were asked to type in both a description of the problem and its underlying cause to ensure that the participant would provide sufficient detail to categorize/code the issue as a cyber or non-cyber issue.

Analogical Intervention. For both the experimental and comparison group, the intervention consisted of reading a passage, structured as a letter from a soldier to his mother, about issues that arose on a fictitious historical mission (circa 1850). The version of the passage presented to the experimental group included historical issues (e.g., carrier pigeon intercepted by enemy) that were intended to be analogous to modern cyber-related issues (e.g., wireless communications signal intercepted/tapped by enemy). The intervention for the comparison group involved a passage describing historical issues (e.g., horse losing a shoe) that were intended to be analogous to modern non-cyber related issues (e.g., vehicle breakdown). Recall that Table 1 summarizes the six historical issues presented in each passage. Note that participants were never exposed to the intended modern analogies. After completing the intervention, the participant then progressed to the post-test (PAT).

RESULTS

To assess whether the analogy intervention was effective, we ran 2(condition: experimental, comparison) by 2(test: pre- vs. post-) mixed ANOVAs for two dependent variables: i) the percent of participants who listed at least one cyber issue; and ii) the percent of cyber (vs. non-cyber) issues listed per participant. These dependent variables are related but we felt that each provided a useful perspective.

Overall, about 54% of participants identified at least one cyber issue on the pre-test. Or, put another way, 46% of participants failed to anticipate any cyber issues on the pre-test. Overall, there was no main effect of test, $F(1, 91) = 0.92$, $pe2 = .01$, $p = .341$, nor condition, $F(1, 91) = 0.05$, $pe2 = .00$, $p = .818$, but as hypothesized, and as shown in Figure 1, there was an interaction, $F(1, 91) = 4.61$, $pe2 = .048$, $p = .034$. In the experimental group, exposure to historical analogies for modern cyber issues significantly increased the percent of participants able to anticipate at least one cyber issue from pre-(49%) to post-test (66%, $p = .030$). In the comparison (physical analogy) group this percentage did not significantly change, and actually numerically decreased, from pre- to post-test ($p = .405$).

In terms of the percent of anticipated issues that were cyber (vs. non-cyber), as above, there was no main effect of condition, $F(1, 91) = 0.10$, $pe^2 = .00$, $p = .756$. However, as hypothesized, there was a significant interaction, $F(1, 91) = 6.05$, $pe^2 = .06$,$p = .016$. In the experimental group (but not the comparison group), the percent of anticipated issues that were cyber increased significantly from pre- to post-test (from 5% to 9%, $p = .002$). This increase in the experimental group drove an overall main effect of test, $F(1, 91) = 4.47$, $pe^2 = .05$,$p = .037$.

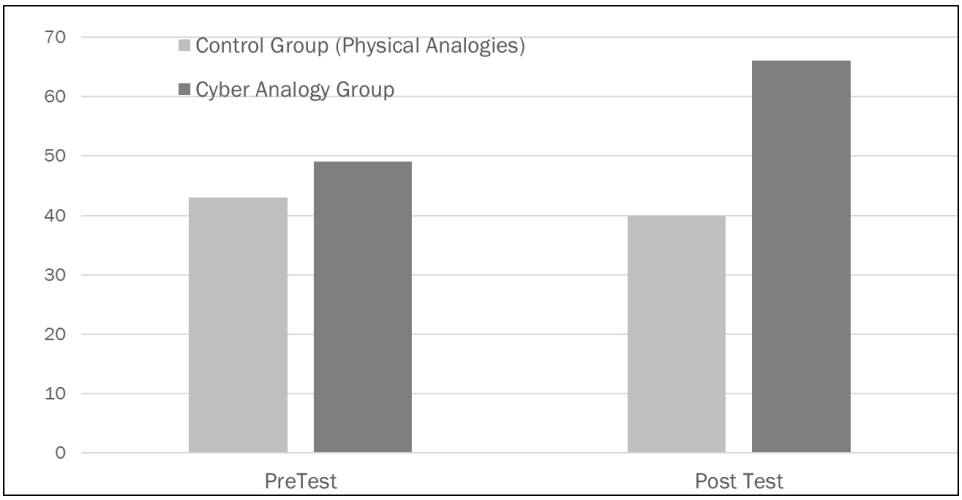

Figure 1: Percent of participants who anticipated at least one cyber/electronic warfare issue.

CONCLUSION

To ensure readiness in the context of multi-domain operations, it is important for all military personnel to be aware of tactical cyber vulnerabilities. Our pre-test results from the Problem Anticipation Task (PAT) indicate that there is some room for improvement in future Army Officers' ability to anticipate potential cyber threats in tactical contexts, which is consistent with results from Pyke et al. (in press). In the prior study, 39% of subjects did not anticipate a single cyber threat, and in the current study (pre-test), 46% did not anticipate a single cyber threat. The current study extended the prior research by developing an effective intervention to improve the ability to anticipate such threats. To compensate for the fact that cyber attackers are often unseen, and cyberattacks often involve invisible wireless signal vectors, our intervention increased the salience of such threats by exposing participants to a passage crafted to contain concrete historical analogies (e.g., carrier pigeon getting intercepted) for modern cyber threats (e.g., wireless signal getting intercepted). These concrete analogies increased participants ability to anticipate modern cyber threats (from under 50% of participants on the pre-test to 66% on the post-test).

DISCLAIMER

The views expressed in this work are those of the author(s) 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.

REFERENCES

Dunker, K. (1945). On problem solving. Psychological Monographs, 58(5), i–113.

Gick, M. L., & Holyoak, K. J. (1980). Analogical problem solving. Cognitive psychology, 12(3), 306–355.

Heatherly, C. J., & Melendez, I. (2019). Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army. The Cyber Defense Review, 4(1), 63–74.

Hsu, J. (2018, January 01). The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data. Wired Website: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Pyke, A., Ness, J. & Feltner, D. (2023). What types of tactical vulnerabilities do future officers most anticipate: Are cyber as well as non-cyber threats on their radar? Cyber Defense Review, 8(1), 103–117.

Schneier, B. & Wheeler, T. (2021, June 4). Hacked drones and busted logistics are the cyber future of warfare. TechStream Website: https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.

Stones, Catherine, James Stark, Sophie Rutter, and Colin Macduff. "The visual representation of germs: a typology of popular germ depictions." Visual Communication 21, no. 1 (2022): 97–122.