What Types of Tactical Vulnerabilities Do Future Officers Most Anticipate: *Are Cyber as well as Non-Cyber Threats on their Radar?*

Aryn Pyke, Ph.D.
James Ness, Ph.D.
Major Dave Feltner

What Types of Tactical Vulnerabilities do Future Officers Most Anticipate: Are Cyber as well as Non-Cyber Threats on their Radar?

ABSTRACT

Modern multi-domain battle involves not only physical threats like IEDs, but also, increasingly, cyber threats. The enemy may jam or intercept communication signals, or hack electronics including navigation systems and drones. Thus, all military leaders - not just signal/cyber specialists - now require some awareness of tactical cyber resources and vulnerabilities. Physical threats come more readily to mind due to their frequency, and because their effects are so salient to the senses. Cyber threats have less historical precedence and are less 'visible' ("out of sight, out of mind"). We developed a task (Problem Anticipation Task: PAT) to gauge the degree to which future Army officers automatically anticipate cyber as well as non-cyber tactical threats. They read a hypothetical mission description and tried to anticipate up to 25 problems that could arise. The mission description explicitly mentioned several cyber-vulnerable components (e.g., radios, navigation systems, drones, biosensors). Yet 39% of these "digital native" participants failed to list a single cyber issue, and only 8% of anticipated issues were cyber-related. The PAT allowed us to assess a baseline regarding our readiness to anticipate cyber vulnerabilities, and can be used in future to assess the effectiveness of training interventions to raise cyber situational understanding.

Keywords: *anticipating tactical cyber threats, cyber situational understanding, cyber readiness, cyber warfare, multi-domain operations*

Aryn Pyke, Ph.D., is a Cognitive Cyber Research Scientist with the Army Cyber Institute and an Associate Professor in the Engineering Psychology Program at West Point. Her doctorate in Cognitive Science provided an interdisciplinary background for the study of cognition (artificial intelligence and modelling, psychology, linguistics, neuroscience). She also obtained BASc and MASc degrees in Electrical and Computer Engineering. Dr. Pyke's research interests include human-computer interaction and teaming, and STEM (Science, Technology, Engineering and Math) education innovations and interventions, especially those involving visuospatial representations. In the cyber domain, Dr. Pyke's focus is on the human in the loop: cyber situational understanding, the impact of affective responses, usable cyber security, and cyber talent management (assessment, training, and retention). To gain insight on human information processing in cyber and educational contexts, she combines behavioral tasks and measures with one or more of neuroimaging, psychophysiological measures (e.g., heart rate, galvanic skin response), eye-tracking and computational modelling and simulation.

Cyber is a Key Domain in Multi-domain Warfare

In the current era of multi-domain warfare, cyber is one of the five key domains (together with air, land, sea, and space). Of the five domains, we view cyber as the one that will most consistently play a role across engagements. Since engagements will not be siloed within a single domain, and will usually incorporate cyber effects,[1] cyber knowledge and situational understanding should not be siloed within particular units or branches (e.g., cyber, signal, and military intelligence). Rather, for the US to be militarily effective, especially against near peer competitors, it has been suggested that every Soldier should be a Cyber Warrior to some extent.[2] The need for such awareness among all military personnel was highlighted when it was discovered that military base locations were being revealed due to the upload of Soldiers' jogging routes recorded by their personal fitness-tracking devices.[3]

Thus, the demands of multi-domain battle raise two related questions: i) how can we assess our Soldiers' level of awareness of cyber vulnerabilities; and ii) how might we further improve it? A main focus of the present research was to develop a method to assess the ability to anticipate potential cyber vulnerabilities in tactical contexts. Without first establishing such a method, it will not be possible to reliably evaluate any training interventions to improve such cyber awareness. The other key objective of the current study was to determine a current baseline level of cyber awareness in a sample of future Army Officers, who will join a variety of different Army Branches. Such a baseline is necessary to gauge our readiness to anticipate possible cyber vulnerabilities in a multi-domain context, and such baseline information is necessary to evaluate the need (if any) for further education and training initiatives to raise cyber awareness among Soldiers in general.

James Ness, Ph.D., is a human factors engineer at the William J. Hughes Technical Center of the Federal Aviation Administration working in modeling and simulations, recently retired from the U.S. Army in the rank of Colonel assigned as Academy Professor, U.S. Military Academy, West Point. He earned the academic rank of full professor in 2016 and upon retirement, he was awarded professor emeritus of the U.S. Military Academy. Before West Point, he served as Command Inspector General, NATO Training Mission/ Combined Security Training Command - Afghanistan. He earned a Bronze Star for his efforts in reforming the Afghan National Military Hospital and establishing an internal assessment program within the Ministry of Interior. Throughout his military career, COL(R) Ness has had varied assignments in human systems integration. Of particular note is his work which led to changes to safety standards by the American National Standards Institute (ANSI) and the International Commission on Non-Ionizing Radiation Protection (ICNIRP) for long-term viewing of near IR laser sources.

Threat-scape Awareness: A Precursor to Situational Awareness

In the heat of the moment, situational awareness,[4,5] involves perceiving those cues in the environment (Observe), that signal potential threats, comprehending their meaning, predicting what may happen next (Orient), deciding what to do (Decide), and then doing it (Act). Due to this Observe-Orient-Decide-Act iterative sequence, the situational awareness process, initially described by John Boyd, is also known as the OODA loop.[6]

A precursor or pre-requisite for situational awareness, however, is typically an advance awareness of the taxonomy of potential threats that might be encountered – what we are calling the threat-scape. To paraphrase Louis Pasteur – "situational awareness favors the prepared mind." Before even entering the tactical context, one should be armed with rudimentary knowledge of the range of potential threats that might occur – including, importantly, cyber threats. This advance awareness of the threat-scape invariably will facilitate a more thorough and nuanced understanding of environmental cues. For example, someone discovering a seemingly inoperable radio (the cue) who did not first anticipate a threat-scape that includes cyber and electronic warfare (EW) might conclude that the device is malfunctioning. Advance awareness allows for another interpretation — that the signal is being jammed. These different interpretations are associated with different implications and courses of action. Presumably, part of the understanding (Orient) phase may involve proactively seeking additional cues to discriminate among multiple possible interpretations of an initial cue.

Readiness and situational awareness for today's and tomorrow's multi-domain battles mandate a threat-scape mindset in military personnel that includes both cyber and non-cyber threats. The current research sought to gauge the degree to which a sampling of future Army officers was armed with this mindset.

Major Dave Feltner, currently a Battalion Executive Officer at 1-508th Parachute Infantry Regiment (Fury From the Sky!) at Fort Bragg, NC. He recently served as Assistant Professor in the Engineering Psychology Program at West Point. His broad research interests include human-computer interaction, cognitive workload, anthropometrics, and biomechanics. He is passionate about arming Soldiers with the right equipment to fight, win, and survive in combat, and has brought experience as an Infantry Officer to bear in research and to help the Army develop, assess, and field optimal equipment.

Why Cyber Vulnerabilities are Not Always Salient in the Threat-scape

As "digital natives," the incoming generation of Army Officers might be keenly attuned to cyber infrastructure issues and vulnerabilities. However, there are several reasons to expect that cyber vulnerabilities may not readily come to mind. First, frequent use of technologies (e.g., computers, cell phones, GPS systems, and the internet of things) does not always equate to familiarity with the inner workings and vulnerabilities of these technologies and their communication signals. Certainly, those who routinely drive cars are seldom familiar with the underlying technology and the diversity of possible ways a car might fail. Second, the wireless communications signals that support modern warfare and travel to and from radios, satellites, drones, cell towers, Wi-Fi hubs, biosensors, et cetera, are invisible. In comparison to visible/tangible targets (e.g., Soldiers, convoys, and bases), which are vulnerable to kinetic attacks, the invisible communication signal vectors for cyber-attacks are, quite literally, out of sight, and often, therefore, out of mind.

Additionally, as the expansion of cyber's importance as a warfare domain is relatively new, cyber-related threats often do not feature in the war stories and scenarios shared by military instructors and mentors. Cyber threats often are omitted in the scenarios encountered in virtual training simulations like Virtual Battle Space (VBS). That said, Service Academies provide academic courses and majors in areas such as computer science, electrical engineering, and cybersecurity that could shed light on vulnerabilities related to the inner workings and wireless signaling of computing and telecommunications equipment, and thereby contribute to cadets' cyber awareness. There may be some limitations to the impact of such academic instruction, however. First, not all students choose to major in such areas (from 2017 to 2021, only about 7% of graduating West Point cadets had majors within computer science

or electrical engineering). Furthermore, although some coverage of information technology is included in the core curriculum taken by all cadets, these academic courses may seldom highlight the use and vulnerabilities of such technology in tactical contexts.

The Present Research

In the current research, we developed and applied a Problem Anticipation Task (PAT) to gauge the degree to which future officers automatically anticipate cyber along with non-cyber threats in tactical contexts. To gauge the diversity and frequency of the types of tactical issues anticipated, our sample of cadets — all "digital natives" — read a description of a hypothetical tactical mission and were asked to anticipate up to 25 possible problems that could arise. Due to the salience challenges discussed above, we expected that participants would anticipate far fewer (if any) cyber issues than non-cyber issues.

For each issue they anticipated, they were asked whether they just thought of it themselves or if they had heard about a similar issue during class, in the news/social media, or via word of mouth. Our hope was to get some insight into the sources of cadets' awareness of tactical cyber versus physical threats. In this vein, we also sought to test whether juniors/seniors were likely to list more cyber issues than freshman/sophomores, given their greater exposure to course work and military training and mentorship. We also sought to investigate whether Science, Technology, Engineering, and Math (STEM) majors were more likely to list cyber issues than non-STEM majors.

To increase the chances that participants would anticipate cyber issues, mission descriptions explicitly mentioned cyber-vulnerable components (radios, navigation systems, biosensors, satellites, drones, cell phones). Our coding scheme categorized responses into three main types of issues: i) non-cyber issues (e.g., equipment malfunction, physical attacks by enemy); ii) cyber issues (e.g., hacking or signal jamming by enemy) and iii) non-cyber information technology/telecommunications (ITT) issues. Non-cyber-ITT issues are those that involved a possible cyber vector like a radio or drone, but the anticipated problem was not due to a cyberattack but rather from other factors such as weather or terrain-caused signal transmission issues. Segregating non-cyber-ITT from cyber and non-cyber issues helped us get a sense of the participant's awareness of unit reliance on equipment that typically is vulnerable to cyberattacks (e.g., cell phones, radios, GPS systems, drones etc.). If some participants list non-cyber-ITT issues but no cyber issues, this will suggest that they are mindful of some intrinsic imperfections and malfunctions associated with communications and digital equipment, but not as mindful of the possibility of deliberate cyberattacks.

METHOD

Participants

West Point Cadets (N = 79; 34% female; mean age: 19.7 years, SD = 1.9 years) received course

credit for participating. These individuals are slated to become U.S. Army officers. Two were seniors, 20 were juniors, one a sophomore, and 56 were freshmen who had almost completed their second semester. In all, 51% were Social Science/Humanities majors and 49% were STEM majors. Sample demographics should reflect the population demographics at the Academy (69% White, 14% African American, 9% Hispanic, 8% Asian, and less than 1% American Indian/Alaska native or other).

Materials

Participants read one of two brief hypothetical mission scenarios, Mission X (311 words) or Mission Y (313 words), (see Appendix 1). Mission X entailed travel to meet with a leader of a local friendly faction and Mission Y was setting up an observation post. Mission descriptions included a sequence of events, modes of transportation, equipment, references to the enemy, supplies, Soldier health, weather and terrain. Such elements in missions can serve as vectors which are subject to attack or other vulnerabilities. The equipment included information transmission, reception and/or storage: radios, cell phones, biosensors, drones, satellites, databases, and GPS devices (e.g., Blue Force Trackers). Such equipment (and/or associated wireless signals) are all vulnerable to cyberattack.

Procedure

The procedure was implemented on-line via the Qualtrics platform. Stimuli and questions were presented on the screen as black text on a white background. A random number generator was used to assign participants to read either Mission X (N = 44) or Mission Y (N = 35). Prior to the display of the mission description subjects were instructed: *"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."* The mission description was then presented on the screen for the participant to read (self-paced), with reminders at the bottom of the description to consider the full range of different problems that might occur, and that even low-probability possibilities were welcome. We refer to our task as the Problem Anticipation Task (PAT). Participants were asked to foresee at least 12 possible problems that might arise, but they had the opportunity to enter as many as 25.

For each possible problem the participant identified, they were asked to describe both the problem and its underlying cause. Requiring the underlying cause ensured that the participant provided sufficient detail to categorize/code the issue. For example, if a possible problem was that the informant could not be contacted – this issue would be coded differently if the cause was: i) a broken cell phone (equipment malfunction); versus ii) the cell signal being deliberately jammed by the enemy (cyber enemy action); versus iii) the informant being killed by the enemy (kinetic enemy action). Participants were also asked to state whether they had heard of their listed issue from the following possible sources: i) in class; ii) news/social media; iii) word of mouth; or iv) just thought of by themself. The procedure took approximately 30 minutes.

Data Coding Procedure

The issues participants listed were each coded according to a two-level scheme involving a type and a subtype. The three main types of issues were: cyber (e.g., radio signal being jammed by enemy); non-cyber-ITT (e.g., radio malfunctioning); and (other) non-cyber (e.g., vehicle breakdown). Cyber problems are those deliberately caused by the enemy (offensive cyber/EW operations), and typically affect equipment vulnerable to cyber threats, including radios, GPS/BFTs, cell phones, drones, biosensors, etc. The non-cyber-ITT category sought to capture cyber-vulnerable equipment problems not caused by enemy cyber operations. Within the cyber type, subtypes of issues included jamming, tapping/tracking of signals, altering information in signals/databases, destruction, or incapacitation of cyber or communications infrastructure, cyber-induced kinetic effects and other. Subtypes for the non-cyber and non-cyber-ITT issues included, among others: equipment malfunction/damage/loss; supply issues; enemy actions (other than cyber/EW); health issues; and issues with weather and terrain. The full coding scheme is summarized in Table 1. Each participant response (anticipated issue) was coded by two independent coders (one military, one civilian) and all discrepancies were resolved in discussion.

Table 1: Coding scheme to categorize anticipated issues by type and subtype

Type	Subtype	Description
Cyber	Jam	Enemy jams signal (e.g., radio, gps)
	Tap/Track Signal	Enemy detects your signal (location) &/or intercepts information
	Alter Information	Enemy alters your communication signals/databases (e.g., to insert false information/ messages/commands)
	Destroy/Hamper Infrastructure	Enemy destroys/hampers cyber/communications infrastructure (e.g., radio/cell towers, satellites)
	Kinetic Effects	Enemy hacking produces kinetic effects (e.g., allows them to overheat or control physical actions of equipment like drones & autonomous systems in vehicles)
	Other	This other category was not actually needed/used
Non-cyber-ITT	(subtypes overlap with non-cyber subtypes below)	Issues with cyber-vulnerable equipment (e.g,. radios, GPS, cell phones, drones) that aren't caused by enemy cyber/EW operations
Non-Cyber	Enemy-Induced	Enemy spots or attacks you (or allies/informants) or moves to a location you were going to use/traverse (e.g., ambush, IED, any injury/fatality/equipment damage caused by enemy)
	Malfunction/Loss of Equipment	Equipment malfunction/breakdown/damage/loss (not caused by enemy)
	Plan	Problems with initial plan or a change of plan
	Supply Issues	Run out of something (gas, bullets, water etc.)
	Health Issues	Health issues not caused by enemy (e.g., fatigue, illness, injury, overheating)
	Personnel/Training Issues	Inadequate training/human error, poor communication, cultural faux pas, infighting, insubordination, disobedience, toxic leadership, AWOL, traitors...
	Intelligence	Incorrect/incomplete intelligence about enemy, or enemy has intelligence on you (without specifying a cyber means of obtaining such intelligence).
	Weather/Terrain/Transmission	Weather or natural terrain affects cover or visibility or signal transmission, or affects travel (e.g., rain washes out a bridge)
	Locals	Local civilians or informants/alleged allies acting against you or compromised or endangered

Participants sometimes listed more than one type and/or subtype of problem in a single entry, e.g.,

Issue: Can't use cell; Cause: No service due to terrain or enemy is jamming it.

Such entries were split into two:

Issue 1: Can't use cell; Cause1: No service due to terrain.

Issue 2: Can't use cell; Cause2: Enemy is jamming it.

For Issue 1, the type is non-cyber-ITT (involving a cyber-vulnerable vector, a cell phone) and the subtype is weather/terrain. For Issue 2, the type is cyber, and the subtype is jamming. When instances were split as exemplified above, both issues inherited the source(s) identified in the original entry. In a few cases (4 cases = 0.4% of trials), a subject listed the same issue twice or listed an issue so broad/vague it could not be specifically coded. In such cases we excluded the issue from our analyses.

RESULTS

Number of Issues Anticipated by Type

Participants averaged 14.4 issues each for a total of 1140 issues generated (not all distinct). Notably, 39% listed no cyber issues whatever. Of the issues identified, 91.8% were non-cyber issues (to include 27.2% non-cyber-ITT), and cyber issues totaled only 8.2%. Figure 1 displays the percent breakdown of issue types and, within each type, the breakdown by subtype.

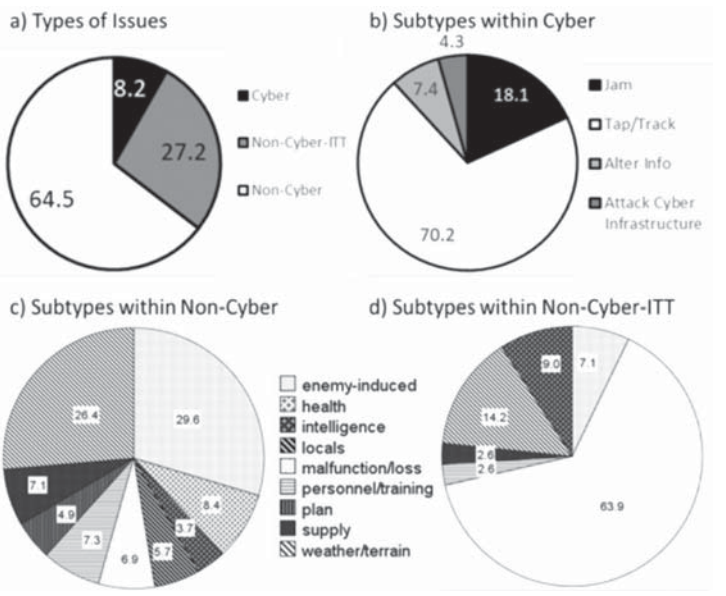

Figure 1. Breakdown of anticipated issues: a) by type; b) by subtypes within cyber; c) by subtypes within the non-cyber-ITT; and d) by sub-type within the non-cyber-other type.

The sample of Computer Science/Electrical Engineering majors was insufficient to allow meaningful comparison with that subgroup specifically, but we did examine whether STEM majors were more likely to list cyber issues than non-STEM majors, and whether juniors/seniors were more likely to list cyber issues than freshmen/sophomores, given their greater exposure to course work and military training and mentorship. For each type of issue (cyber, non-cyber-ITT, non-cyber), we performed a 2 (college level: freshmen/sophomores vs. juniors/seniors) X 2 (type of major: STEM vs. non-STEM) analysis of variance (ANOVA) on the number of potential issues raised by each participant. As summarized in Table 2, the analysis revealed no significant differences by college level nor by major (STEM vs. non-STEM), nor any significant interactions between the two variables. Thus, in this sample at least, there is no significant evidence of significantly increased ability to anticipate more cyber threats (nor more physical threats) among older cadets nor among STEM majors.

Table 2: Mean number of issues listed (per participant) for each type by college level and major.

Issues	Cyber		Non-cyber-ITT		Non-cyber-ITT		Cyber Infrastructure	
College Level	Non-STEM	STEM	Non-STEM	STEM	Non-STEM	STEM	Non-STEM	STEM
Freshman/	1.2	1.2	4.1	4.0	9.2	10.1	14.4	15.2
Sophomores	1.3	1.3	3.5	3.9	8.9	7.7	13.5	12.9
Statistics	**Note: All statistical comparisons failed to reach significance**							
Main effect: College Level	$F(3,75)=0.04$, $p=.845$		$F(3,75)=0.43$, $p=.512$		$F(3,75)=2.39$, $p=.126$		$F(3,75)=3.15$, $p=.080$*	
Main effect: Major	$F(3,75)=0.02$, $p=.893$		$F(3,75)=0.10$, $p=.749$		$F(3,75)=0.04$, $p=.845$		$F(3,75)=0.01$, $p=.937$	
Interaction	$F(3,75)=0.16$, $p=.689$		$F(3,75)=0.21$, $p=.649$		$F(3,75)=1.55$, $p=.217$		$F(3,75)=0.65$, $p=.423$	

** Significant p-values are those <.05, Freshman/Sophomores listed marginally (p<.1) more issues overall (but not in cyber) than Juniors/Seniors.*

Cyber Threats Anticipated: Subtypes and Vectors

Figure 1 illustrates that the most common subtype of cyber issue anticipated was that the enemy would tap or track a signal (70.2% of cyber issues raised), which corresponds to compromising the *confidentiality* aspect of cybersecurity. The next most anticipated issue was an enemy jamming a signal (18.1%), compromising *availability*. The third most anticipated issue was the enemy-alteration of a signal or stored/displayed information (7.4%), which corresponds to the information *integrity* aspect of cyber security. Fourth was an enemy physically destroying cyber infrastructure (4.3%), which, like signal jamming, also relates to information *availability* (for a total of 22.4% availability issues). Our pre-experimental coding scheme also included a code for a cyberattack with kinetic effects (e.g., enemy hacking a drone and directing it to fly into a friendly Soldier or vehicle), but our participants did not list any such examples. In terms of which vectors (e.g., pieces of equipment, signals) were most anticipated as cyberattack targets, the most frequently mentioned was a cell phone, followed in order by the GPS, the radio/comms, and the drones and biosensors.

Table 3 associates different vectors (e.g., pieces of equipment) with the distribution of subtypes of issues that cadets anticipated might arise for that vector. Note, the unbracketed percentages are percentages just within the subset of issues associated with a particular vector (column). For example, issues with drones (N=58) amounted to 5% of the total cyber and non-cyber-ITT issues. Only 15% of the 58 issues associated with drones were cyber issues, and the rest were non-cyber-ITT issues (e.g., equipment malfunction).

Table 3: Percent of anticipated cyber (grey background) and non-cyber-ITT (white background) problems associated with different pieces of cyber-vulnerable equipment.

Issues	Drone	Navigation System	Bio-sensor	Radio/Comms	Cell Phone	Cyber Infrastructure
Number Issues	N=58	N=99	N=64	N=78	N=86	
Cyber						
Jam	None	3% (18%)	5% (18%)	8% (35%)	6% (29%)	n/a
Tap/Track	5% (5%)	16% (24%)	9% (9%)	13% (15%)	36% (47%)	n/a
Alter Info	5% (43%)	4% (57%)	none	none	None	n/a
Kinetic Effects	none	none	none	none	None	n/a
Attack Cyber Infrastructure	5% (75%)	n/a	n/a	n/a	n/a	1% (25%)
Total Cyber	15%	23%	14%	21%	42%	1%
Non-Cyber-ITT						
Enemy (spots/damages)	22%	1%	2%	none	1%	(coded as cyber)
Malfunction	17%	62%	77%	58%	34%	n/a
Supply/Batteries	none	1%	none	8%	1%	n/a
Weather/Terrain	9%	9%	3%	10%	21%	n/a
Personnel/Training	none	2%	5%	1%	none	n/a

Note: Un-bracketed percentages reflect responses of that subtype within that column (equipment type), and percentages in round brackets are the percentages of that subtype within that row.

Non-Cyber Threats Anticipated: Subtypes and Vectors

Part (c) of Figure 1 above breaks down the subtypes of non-cyber issues listed by participants, to show the percentage of issues in terms of the most common attack surfaces and/or aspects implicated: route/visibility (31.0%), Soldiers (21.9%), local informant/ally (12%), plan/preparation/support (9.8%), vehicles (8.6%), weapons/ammunition (4.1%), and other equipment (1.6%).

Sources of Participants' Ideas about Possible Issues: Were any mentioned in class?

For each issue flagged, cadets were asked to identify whether they had previously heard of this possible issue by checking all that applied from the following possible sources: i) classroom; ii) news/social media; iii) word of mouth; or iv) thought of by the cadet without outside prompting. The data were coded so that unprompted issues were those where only that source was checked and no other. It is hard to claim that you just thought of something yourself if you also stated that you had heard it mentioned in class, and/or in the news or social media, and/or

via word of mouth. Figure 2 shows the proportion of participants who cited each possible source for the issues they listed by type (cyber, non-cyber-ITT and non-cyber). Since only 61% of participants listed a cyber issue, values in the cyber category can't exceed that percentage.

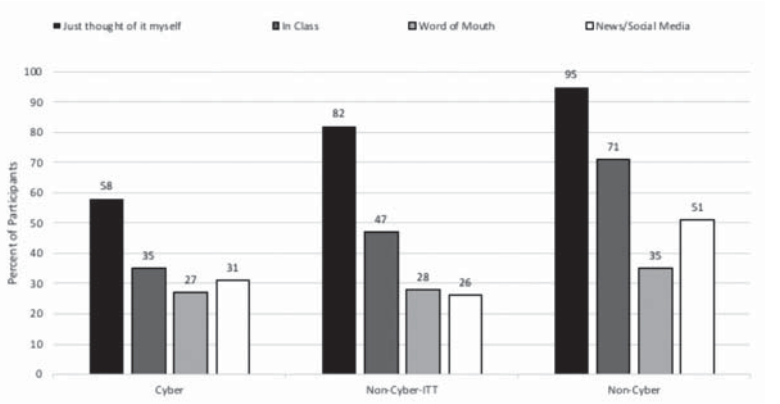

Figure 2: Percent of participants citing various (non-exclusive) sources for anticipated issues, separated by issue type.

For several reasons we predicted that cadets might anticipate fewer cyber issues. First, they have less historical precedent than non-cyber issues, and may be less likely to be mentioned in class or via word of mouth by military mentors. In contrast to the 71% of participants who attributed anticipating one or more non-cyber issues to in-class exposure, only 35% of participants attributed anticipating a cyber issue to in-class exposure. Word-of-mouth attributions were also lower for cyber than non-cyber issues. Second, not all students are familiar with the workings of cyber technology, which renders 'invisible' cyber threats more abstract and hence more difficult to picture than, say, an explosion. This view is consistent with our finding that, compared to the 95% who came up with non-cyber issues themselves (without exposure to any external source), only 58% reported coming up with a cyber issue themselves.

DISCUSSION AND CONCLUSION

In this research we developed a methodology to assess a type of cyber awareness relevant to multi-domain battle - i.e., the ability to anticipate both cyber and physical vulnerabilities in a tactical context, because situational awareness on today's battlefield demands both. It is necessary to be aware, in advance, of the types of problems that could occur (Threat-scape Awareness), as preparation to be aware of cues in the heat of the moment that a particular problem might be occurring right now (Situational Awareness).

Overall, only 8% of anticipated problems were cyber related, and 39% of participants anticipated no cyber issues at all. Thus, despite our subjects being "digital natives," potential cyber issues were not even on the radar for many of these future Army officers. That said, being digital natives likely did facilitate cadets' ability to anticipate non-cyber-ITT issues like malfunction,

human error, and battery supply associated with equipment like radios, drones, cell phones etc. Our results are compatible with research on mobile device use in civilian contexts, which suggests that many digital natives lack high cyber security awareness,[7] and they need education and/or training to inculcate cyber security awareness.

In terms of education and training, a surprising finding – and concern - is that, in this sample at least, neither older cadets nor STEM majors evidenced an increased ability to anticipate more tactical cyber threats. West Point is increasing opportunities for both curricular and extra-curricular exposure to cyber-related content. In terms of the curriculum, all cadets, regardless of major, must take two core internet technology courses, and a 3-course engineering sequence, and one of the six options is Cyber Engineering. The Department of Computer Science and Electrical Engineering offers three majors for interested cadets: Computer Science, Electrical Engineering, and a recently added Cyber Science Major. A Cyber Engineering Minor is also offered. Several other departments have also offered cyber-related elective courses (e.g., Cyber Policy, Cyber Law, Cyber History), which are often developed and/or taught by faculty from the Army Cyber Institute. In addition, extra-curricular opportunities include a cyber leader development program where cadets may earn a cyber skill identifier, as well as several cyber-related clubs and teams, e.g., the Cadet Competitive Cyber Team (C3T), Cyber Policy Team, Esports Team, Electrical Engineering Systers Club, Amateur Radio Club, Electronic Experimenters' Group, Association for Computing Machinery Student Chapter (ACM-SIGSAC), and more.

We expect that West Point is not unique among the service academies in offering such opportunities, yet it would not surprise us to learn that our counterparts also may come up short in ready awareness of potential tactical cyber threats and vulnerabilities. Again, we envision two plausible reasons for this. First, beyond core required internet/cyber courses, not all students will engage with the available opportunities. Second, academic courses on cyber-related content may not touch on tactical cyber threats and vulnerabilities. An example of an exception at West Point was an engineering psychology colloquium on Human-Computer-Interaction, developed and taught by the second author, which involved brainstorming and story-boarding ways to include cyber threats into scenarios in a video-game-like military training simulation platform called Virtual Battle Space (VBS). Due to faculty turnover and availability, however, specialty and elective courses may not always be systematically available.

Beyond the academic curriculum, tactical cyber issues could be more directly addressed in the military instruction and training components of the cadet experience. We acknowledge that only two cadets in our sample were seniors, and further, that their post-graduation level of awareness of cyber and EW threat vectors could be enhanced by branch Basic Officer Leader Course (BOLC) training. That said, we suspect that many BOLC courses for non-cyber officers may include minimal cyber content, and so it is an open question whether a Problem Anticipation Task (PAT) administered post-BOLC would yield results much different from those reported here.

Recommendations and Future Work

An obvious extension of the current work would be to apply our PAT methodology to gauge tactical cyber awareness in other services and stages of training or career development. In the Army, this could include, for example, before and after each institutional professional education course (e.g., BOLC and ILE: Intermediate Level Education). Beyond assessing current awareness, the PAT can also be used as a pre-/post-test to assess the effectiveness of inserting additional cyber content into professional military education courses.

More narrowly, within the West Point context, a core required cyber course or military instruction course could be modified to include a section on tactical implications of cyber threats and vulnerabilities, to ensure exposure for every student. One could take a training approach and explicitly spell out several specific examples (i.e., give someone a fish). Or, taking a more educational approach, we could provide students an example and encourage them to apply and generalize their (non-tactical) cyber knowledge to generate other potential cyber issues (i.e., teaching them to fish). This could be done in the context of the task used in this study (PAT). Research indicates that students better retain/recall content they helped to generate versus content that was presented to them.[8,9] Participants engaged in this generation process in the current study when they reported the source of their issue idea as "just thought of it myself." Beyond the benefits of better retention/recall (of known threats), this generation process is crucial to enabling anticipation of potential novel/future threats that could emerge in the evolving, multi-domain context of modern warfare.

The "invisible," and hence more abstract nature of cyber threats will always be a challenge. To ameliorate this, the military is actively researching and developing interfaces to better support cyber understanding for leaders. Such interfaces might visually represent not only the physical assets and aspects of an area but also, potentially, cyber resources, signals and interconnectivity. Visual representations might also support better understanding for students in the classroom. This is an area for continued, on-going research.

APPENDIX 1: PARAGRAPH DESCRIPTIONS OF HYPOTHETICAL MISSIONS

Mission X: The goal of your Platoon (PLT) is to meet with a leader of a US-friendly faction in the region. You'll start at a Forward Operating Base (FOB). After a quick medical check, you will travel 65 miles via Stryker ground vehicles to the meeting point. The current forecast predicts good weather. Your planned route will take advantage of the local roads and bridges, but to avoid engagement, your route will detour around regions that seem to be occupied by hostile forces - based on reconnaissance images transmitted wirelessly by Drones. Thus, you will detour across a river to travel 25 miles on the far side and then cross back again. In addition to rations, each Soldier in your unit will still carry an M4 with a full ammo load, and the Strykers will be equipped with machine guns and a 60mm Mortar system. Each Stryker is also equipped

with a Situational Awareness Navigation system (Blue Force Tracker: BFT), which has GPS and satellite communication capabilities and displays a route map with information on your position, destination, the positions of other vehicles in your unit, and expected positions of the enemy forces based on the most recent intel. There are actually two possible meet locations (A and B). When your unit is about 20 minutes out from the meet, you (the PL) will contact the local faction leader via cell phone to determine which meeting site to use. You will then communicate this information by radio to members of your PLT in the other Strykers and to company HQ. When you arrive at the final meet site, you and the Platoon Sergeant (PSG) will dismount the Stryker to walk across the clearing to meet the local leader. Your PLT and company HQ can still monitor your well-being remotely because all Soldiers will be equipped with biomedical sensors that track their vitals and position.

Mission Y: The goal of your Platoon (PLT) is to set up an observation post to detect enemy movements along a particular route. You will start from a forward operating base (FOB). After a quick medical check, and after packing rations, observation equipment, M4s and a full ammo load, your unit will be flown at night by C-130 aircraft to parachute into an area several miles from your destination. This should minimize the likelihood that hostile forces will detect your movements. You will then navigate on foot using satellite-enabled GPS to a site on a ridge overlooking the route to be observed. The GPS will provide a route map with information on your position, destination, and the positions of other members in your unit. Your ruck to the ridge will involve crossing a riverbed that should be dry at this time of year. Your observation site on the ridge was selected based on images transmitted wirelessly by Drones that indicate that it is not occupied by enemy forces and will provide you with ample cover due to rock formations and vegetation. It should also provide an excellent line of sight to the target route if the good weather/visibility holds. If enemy movement is detected along the target route, you'll immediately communicate this information via radio to company HQ at the FOB. You also have a cell phone which can allow you to receive intel from a local informant who can give you advance warning if your position has been compromised or if the enemy is making unexpected movements in the region. Besides keeping watch from the observation post, you will also periodically send a squad out to do a foot patrol of the area. The PLT and company HQ can monitor the well-being of Soldiers on patrol because all Soldiers will be equipped with biomedical sensors that track their vitals and position.

DISCLAIMER

The views expressed here are exclusively those of the authors 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. Correspondence concerning this article should be addressed to Aryn A. Pyke, Army Cyber Institute, 2101 New South Post Rd, U.S. Military Academy, West Point, NY 10996. Email: aryn.pyke@westpoint.edu.

NOTES

1. Bruce Schneier and Tarah Wheeler, “Hacked drones and busted logistics and the cyber future of warfare”. TechStream, June 4, 2021, https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.
2. Christopher J. Heatherly and Ian Melendez. "Every soldier a cyber warrior." *The Cyber Defense Review* 4, no. 1 (2019): 63-74.
3. Jeremy Hsu, “The Strava Heat Map and the End of Secrets.” *Wired*, January 9. 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
4. Mica R. Endsley, "Measurement of situation awareness in dynamic systems." *Human factors* 37, no. 1 (1995): 65-84.
5. Mica R. Endsley, "Design and evaluation for situation awareness enhancement." In *Proceedings of the Human Factors Society annual meeting*, vol. 32, no. 2, 97-101, Los Angeles, CA: Sage Publications, 1988.
6. Chet Richards, “Boyd’s OODA Loop” *NECESSE* (Royal Norwegian Naval Academy Monographic Series), February 11, 2020, https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2683228/Boyds%20OODA%20Loop%20Necesse%20vol%205%20nr%201.pdf?sequence=1&isAllowed=y.
7. Vasileios Gkioulos, Gaute Wangen, Sokratis K. Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou, "Security awareness of the digital natives." *Information* 8, no. 2 (2017): 42.
8. Norman J. Slamecka and Peter Graf, "The generation effect: Delineation of a phenomenon," *Journal of Experimental Psychology: Human Learning and Memory* 4, no. 6 (1978): 592.
9. Aryn A. Pyke and Jo-Anne LeFevre, "Calculator use need not undermine direct-access ability: The roles of retrieval, calculation, and calculator use in the acquisition of arithmetic facts," *Journal of Educational Psychology* 103, no. 3 (2011): 607.