Security Mindset Fundamentals and Second Language Learning

Amy Kuiken
School of Education
Wilkes University
Wilkes-Barre, PA, USA
0000-0002-8100-7639

***Abstract*—Security mindsets can be said to engage elements of situational awareness and analytical, creative, and practical elements of adversarial thinking. Scholars have debated whether this is taught or fostered, but they have acknowledged that security mindsets are critical. Here, the argument is made that implicit features of language itself can be drawn on in everyday K12+ second language (L2) learning settings to introduce members of the general populace and, among them, potential future members of the cybersecurity workforce, to security thinking. Beyond the features of language itself, L2 lessons can also be adapted to familiarize students with explicit security-related topics and scenarios. By exploiting these novel connections between language learning and security thinking, L2 learning contexts can become a security mindset training ground for millions of U.S. students.**

Keywords—security mindset, adversarial thinking, situational awareness, second language learning, K12+, cybersecurity for non-cyber students, inclusion and diversity

I. Introduction

Cybersecurity education has long faced the challenge of responding to an ever-evolving cybersecurity landscape [1], [2]. Experts have asserted that past educational practices are insufficient for keeping pace and have called for a variety of new approaches [3]. In what follows, I explore a novel approach related to developing security mindsets. I begin by situating security mindsets in the context of cybersecurity education before exploring potential links between security mindsets and second language (L2) learning. I conclude with preliminary thoughts on how to leverage these links in L2 learning settings.

A. Past Practice

Cybersecurity education in the U.S. has historically been rooted in programs separate from the rest of the curriculum [4] and have generally treated cybersecurity as a specialized, technical problem [5]. This "technification" [6] of cybersecurity arguably left the cybersecurity workforce with strong analytical and technical skills but weaker creative and practical skills [7]. In addition, introductory programming and cybersecurity courses often prioritized software over security [3]. Taken together, a picture of cybersecurity education emerges where human elements were largely overlooked and security presented as an afterthought.

B. Present Calls for Change

While scholars still highlight the need for technical training to keep pace with changes (e.g., [3], [8]) there is also recognition that the fundamentals of security are not technical but human [9] - [12]. In addition, [7. p. 10] observed that "although today's cybercrime is worlds apart from the hacking of the 1980's…the fundamental techniques…have not changed." A push to focus on enduring security principles has therefore been gaining traction among cybersecurity thinkers (e.g., [3], [9], [13], [14]) and [3, p. 2] asserted that "teaching the 'security mindset' might be one of the most important aspects" of cybersecurity education today.

II. Security Mindsets

A. In Search of a Definition

What constitutes a security mindset[1] and the terminology referring to it has been somewhat fluid [13], [15]. Security mindset concepts have surfaced under the guise of cybersecurity critical thinking [16], cybersecurity situational awareness [17], and adversarial thinking [7], [18]. It has also been presented in terms of imagining how things might fail or be exploited [19]. Severance [9, p. 8] equated a security mindset with attempting "to understand the unexpected directions from which attacks might come." Katz [18, p. 15] suggested that a security mindset meant "anticipat[ing] the strategic actions of others." Nassiokas [20, para. 3] described it as "noticing anomalies or 'things that don't fit' in a specific scenario or context" while [21, p. 72] identified the need for having "open and adaptive" mindsets to understand the explorative and exploitative aspects of hackers' mindsets.

Security mindsets have been framed by thinkers and practitioners as the ability to think like a hacker [9], [22], although [13] and [7] found this problematic. Hamman and Hopkinson [7] pushed for a more precise characterization. They suggested instead that such thinking entailed "the ability to approach system rules, operational spaces, and player actions from a hacker's perspective" [7, p. 6] and drew on Sternberg's Theory of Triarchic Intelligence [23] to

[1] Security mindsets are typically referred to in the singular as *security mindset*. I am grateful to Jane Blanken-Webb for her insight that there is no single mindset that constitutes security thinking; to reflect this, I have opted to use the plural whenever possible.

identify analytical, creative, and practical components of adversarial thinking.

While [7]'s work offers a valuable tool for understanding fundamental components of security thinking, [5, p. 4] suggested that approaching these more qualitatively could help further define and operationalize such "a complex set of concrete habits, values and attitudes." Here, I submit that conceptions of situational awareness (e.g., [24] - [26]) complement understandings of how [7]'s security mindset components work together in concrete contexts. Hailed by one risk management company as foundational to a security mindset [27], situational awareness encapsulates a process of perceiving, comprehending, and projecting [24].

Horneman [26, para. 9] aimed to render [24]'s model of situational awareness more practical for cyberspace, summarizing it as "1. Know what should be. 2. Track what is. 3. Infer when *should be* and *is* do not match. 4. Do something about the differences." By viewing adversarial thinking capabilities through this lens, a dynamic big picture emerges wherein understanding depends on weighing outside information against "knowledge and goals, which in turn informs the projected status of the world" [25, p. 6].

For the purposes of this discussion, security mindsets are defined as an ingrained habit of investigating and identifying how things (including people, systems, and processes) can fail. Used interchangeably in this paper with *security thinking*, security mindsets can be said to engage components of situational awareness and adversarial thinking, with these informed by domain-specific knowledge and skills. In drawing on aspects of both [7]'s and [24]'s frameworks, a picture emerges of not only specific capacities but of the interplay between them (Fig. 1). These elements work together to protect the penultimate concerns of security that make up the security triad: confidentiality, integrity, and availability.

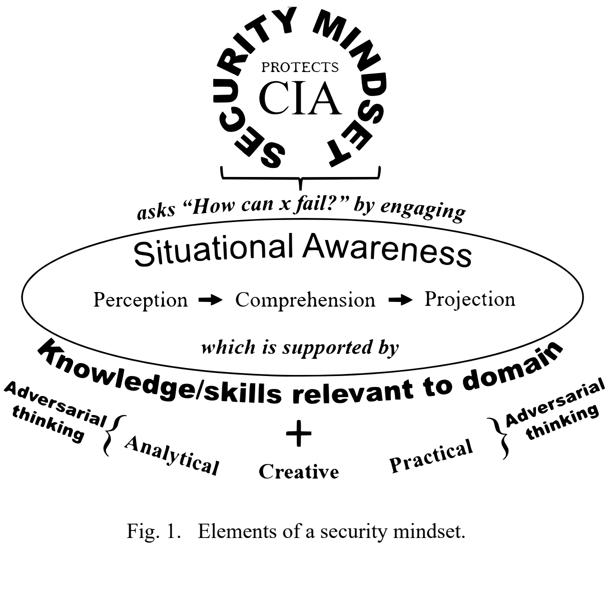

Fig. 1. Elements of a security mindset.

B. Teaching Security Mindsets

Dark [28, p. 61] wrote that "when cybersecurity educators talk about what graduates need to know, the answer is often summarized in two words: security mindset." The difficulty, however, is that there is a lack of attention paid to security mindsets fundamentals in existing textbooks [9]. Moreover, scholars have questioned whether security mindsets can even be taught [3]. Hamilton [3] felt that building security mindsets in everyone would ultimately be unfeasible, as most people never pursue careers requiring deep technical skills and thus few will ever grasp the true nature of cyberthreats. Schneier [19] speculated that teaching security mindsets was potentially far more difficult than teaching domain-related knowledge. Dark [28] doubted if it were possible to teach students how to identify and handle ambiguous, complex, and dynamic situations in traditional instructional settings.

Dark [28] also maintained, however, that in reimagining schools as places of experiential learning, this kind of thinking could be fostered. Others have expressed even more optimism: [29] reported finding an effective strategy for developing learners' security thinking using an adversarial teaching approach. Hamman and Hopkinson [7] argued that certain aspects of security thinking could be developed in students by tying them to specific learning outcomes for the benefit of cybersecurity educators. While [7] questioned if creative thinking could be developed (or simply identified) in students, they held that students' practical reasoning could indeed be improved through instruction. Kaza [3, p. 2], who also championed the possibility of teaching security mindsets, called for "a deliberate effort," urging for currently-taught topics to be supplemented with security-related resources.

The call for deliberate teaching aligns with critical thinking pedagogy [30]. Given that security mindsets may be characterized as a specific kind of critical thinking [31], [32], educators would do well to note that students' critical thinking skills can be developed [30], [33] and that at least some explicit instruction has been found to be necessary [30]. In addition, the potential for developing critical thinking and transferring it to other contexts is boosted when real-life settings are applied [30]. This transfer is valuable in a rapidly shifting cybersecurity landscape.

With this in mind – that developing students' security mindsets is of critical concern and that fostering security thinking is possible – I move on to explore a potential means for addressing the challenge.

III. SECOND LANGUAGE LEARNING AND SECURITY MINDSET FUNDAMENTALS

In what follows, I make the claim that content and processes in K12+ language learning classrooms are particularly well-suited to meet the challenge of developing students' foundational security thinking. Second language (L2) learning instructional settings – including foreign language (FL), English language learning (ELL), and sign language – can provide a security mindset "training ground" in multiple ways.

A. *Exploiting Features of Language*

One way that L2 settings can foster students' security mindsets hinges on the fact that languages themselves are rule-governed [34], creative [35], and practical [36]. This corresponds neatly to [7]'s basic elements of adversarial thinking. Of course, learners can practice their analytical, creative, and practical skills without any thought to adversarial thinking (as current anecdotal evidence in L2 classrooms suggests). However, my concern here is to identify promising links between security mindset themes and features of L2 learning that could be leveraged by materials designers and practitioners to develop students' security thinking. Below, I explore opportunities for students to exercise their analytical, creative, and practical intelligences in ways that specifically engage security mindset fundamentals.

1) Fostering analytical capacities: Language is a rule-governed and protocol-rich system made up of phonetic/phonological, morphological, syntactic, semantic, and pragmatic subsystems [37]. While these subsystems can be subjected to intense analysis, speakers may not be consciously aware of this structure at all when learning their native tongues. L2 learners, on the other hand, are presented with a second chance to attend to language's fundamental features [38]; L2 materials often highlight different subsystems of language with sections dedicated to explaining and practicing pronunciation, grammar and vocabulary, and social contexts. Whether students are explicitly taught – or merely exposed to – these subsystems in L2 settings, engagement with them requires knowledge of rules and systems on some level [39]. Here, one finds in-roads for developing students' analytical capabilities more consciously. Students can begin to identify elements needed to build a successful message, while pattern recognition, outlier identification, and disambiguation are brought within learners' reach. When coached to attend to technical and procedural concepts in language, students can identify threats to the integrity and availability of their messages – in experiencing how failure to apply a rule may inadvertently alter a message or render its meaning unavailable to their audience. Given that a speaker's inattention, fatigue, or lack of training can result in communication failure, it may even be possible for L2 learners to take the view of themselves as the benign inside threat in their attempt to apply rules. Table I connects some examples of typical L2 learning content with recommendations from the literature for fostering analytical capabilities.

TABLE I. ANALYTICAL LINKS

Recommendation for supporting analytical security thinking	**L2 learning content and practices that can be leveraged**
Familiarity with systems, rules, and protocols [7].	-Pronunciation rules, spelling rules, verb conjugations, noun declensions, sentence structure, social protocols, etc. *Example: When teaching letter combinations (e.g., ou, pf, ent, ll), teachers underscore that 1) the L2 system has its own rules, 2) knowing rules is key for using the system, and 3) changing one thing can have consequences: if mispronouncing "ou" in "merci beaucoup," students risk complimenting a listener's buttocks rather than saying "thank you."*
Putting together or breaking apart components [7]	-Attaching/separating prefixes and suffixes to/from root stems, pulling out parts of sentences to substitute with other parts according to linguistic formulae *Example: When teaching French negation, the teacher shows students how to insert grammatical components into statements to completely alter their meaning.*

2) Fostering creative capacities: If analytical intelligence means a facility for identifying and implementing rules in a system, creativity means a facility for identifying ways to exploit the rules [7]. Language is a creative system steeped in novelty with respect to combining words and rules [37], [42], [43] and L2 learning settings often entail encountering novel social conventions and contexts as well. Because L2 learners "need to learn new patterns…[and] appropriate new ways of thinking about what they perceive as established and taken for granted" [30, p. 55], it is unsurprising that exposure to other languages has been found to increase learners' creativity [44]. I suggest that by providing (or not providing) spaces for students to take creative risks with the target language to bend and break the rules, L2 instructors may greatly influence the extent to which students exercise creative intelligence.[2] Table II connects typical L2 learning content to recommendations from the literature for fostering creativity with regard to security thinking.

[2] Anecdotally, I have observed L2 students' creativity in at least two ways: 1) playing within L2 rules and 2) intentionally bending or breaking the rules. While neither has to be done adversarially, I suggest both can enhance security thinking.

TABLE II. CREATIVE LINKS

Recommendation for supporting analytical security thinking	**L2 learning content and practices that can be leveraged**
Exposure to novel / unconventional perspectives [7], making "unique connections and see[ing] the world in original ways" [7, p. 6]	• Novel sounds, words, rules, behaviors, and attitudes • Lack of equivalency of concepts *Example: Teachers point out to French students that some dialects have no word for 70, but it is expressed by "sixty-ten." The teacher helps students consider how this alternate way to "do" numbers challenges them to reexamine concepts previously taken for granted, and how this helps them look out for potential future "surprises."*
Imagining unorthodox responses [7]	• Exercises inviting unique responses rather than relying exclusively on predetermined "correct" responses • Dialogues that go off-script • Exercises that don't penalize mistakes made by experimenting *Example: In asking students to create a basic dialogue with greetings, teachers can allow them freedom to experiment and formulate their own dialogues based on (but not bound to) provided examples. Teachers can point to how departing from the standard script is one way hackers experiment with using old rules to do unexpected things.*
Putting old things together in new ways [7], manipulating / subverting system rules to create novel outcomes [45]	• Combining sounds/words/ phrases/gestures in previously unmodelled/unprescribed ways • Conjunctions *and/or* as a tool for building infinite loops • Intentionally using informal language when formal is required (or vice versa) to tinker with social dynamics *Example: When teaching "and" and "or," the teacher can highlight how students now have a way to extend phrases ad infinitum. With only a few basic words, students can create unique utterances possibly never said before. Teacher draws attention to the creative value of asking "What can be done with what I have?" – a typical way of thinking for hackers.*
Exposure to open-ended challenges [9]	• Language situations where multiple utterances are possible *Example: Teachers can encourage student creativity through lessons using "what" and "why" and underscore how security questions are often open-ended.*

3) Fostering practical capacities: Language is practical whenever it has "a direct bearing on what we want and plan to do" [36, p. 1]. When giving commands or making judgments, speakers employ practical aspects of language [36]. In such speech acts, speakers endeavor to adapt, shape, and select elements of their environment – core aspects of social engineering where hackers employ any number of strategies to achieve their goals [7]. In settings mediated chiefly by language such as email or texts, social engineering may involve linguistic politeness strategies in addition to other tactics used by hackers, such as pretexting [46]. When L2 learners are taught about formality, greeting protocols, and politeness strategies, they are in fact learning to recognize and use tools in a hacker's repertoire. Table III presents recommendations from the literature relevant to developing learners' practical capabilities and provides examples of content in L2 learning settings which could be used to those ends.

TABLE III. PRACTICAL LINKS

Recommendation for supporting analytical security thinking	**L2 learning content and practices that can be leveraged**
Exposure to using/opportunity to use "social and communication skills that enable them to [get] people to release essential information or to perform critical actions" [21, p. 72]	• Politeness strategies such as greetings, using formal / informal language to be respectful/friendly • Adopting a different persona for different conversations *Example: When teaching different strategies for greeting people, teachers can help students evaluate the impact of using formal language to show respect and informal language to show familiarity. Teachers can help students think about how each is used in social engineering.*
Fitting in/evading detection [7]	• Learning physical gestures • Issues of pronunciation/accent/ regional variation in vocabulary *Example: In a dialogue scene where students read from scripts, teachers can help students consider how their speech and behaviors might change when playing the role of a child, neighbor, or senior, and how attackers do this to blend in.*

Recommendation for supporting analytical security thinking	**L2 learning content and practices that can be leveraged**
Attending to the motivation of others/anticipating actions [7], [18]	- Anticipating what others will say *Example: When presenting a scripted dialogue, the teacher can ask students to guess what the next line is in the dialogue before seeing what actually comes next. The teacher helps students consider the likelihood and appropriateness of various responses and connect this skill to security thinking.*
Viewing exchanges in terms of adversaries [9]	- “Flipping the script” on dialogues typically set up to be between friends *Example: Teachers can take any textbook exercise that is a dialogue set between friends and ask students to imagine how the interaction might change if one of the speakers is attempting to steal information or provide inaccurate information.*
Being exposed to the consequences of one’s own errors [3]	- Attending to feedback from listeners/readers/instructors to find out how successful communication was - Managing miscommunication *Example: Teachers can indicate to students when they fail to get parts of their message across, and help troubleshoot where the failure occurred (pronunciation, grammar, word choice, gestures, loudness, etc.). Students can consider how consequences can change depending on the message’s value.*
Strategic reasoning in scenarios with multiple actors, accounting for others’ possible behavior and anticipating how various strategies would play out [47]	- Multi-person improv - Dialogues with complex plots *Example: Teachers can invite students to create a skit with multiple characters interacting. The teacher directs students’ attention to imagining possible outcomes between characters; students can present multiple versions and consider the likelihood of certain events.*

4) Fostering situational awareness: Language is situated [48]. L2 instruction can foster students’ security mindsets by capitalizing on this feature. Indeed, L2 curricular materials already do this when including information about cultures and places, and textbooks can provide background information or context to introduce dialogue scenes and other activities (e.g., [49], [50]). Conscious attention to the sum of these details can open the door for students to make sociolinguistic judgments about which utterances and behaviors are optimal in a given context. This can be extended further by directing students to gather clues about trustworthiness or likelihood of events. When conversations are situated in a context (e.g., “You are on your way to an afternoon party when you see your classmate Françoise sitting at a café”), L2 instructors have numerous opportunities they can leverage to direct students’ attention to factors that could impede communication or lead to undesirable outcomes (e.g., “Is the café crowded? What could a pickpocket get from you? Is it important to know the time of day when greeting in French? How do you pronounce Françoise’s name to avoid misgendering her?”) Attending to situational details can point students toward notions of data type and value as well, raising awareness about appropriate contexts for sharing. As students perceive, comprehend, and project in (simulated or real) novel situations – drawing on analytical, creative, and practical capabilities – their information-gathering and decision-making skills can become routine.

Situational awareness can also be invoked at more technical levels. Learners perceive and comprehend language mechanics with varying degrees of awareness [51]. Here, awareness refers to “explicit knowledge about language, and conscious perception and sensitivity in language learning…and…use” [52, para. 1]. Horneman’s [26, para 9] notion of knowing “what should be” would seem to apply to learners’ efforts to gather this explicit knowledge about language. The fact that L2 learning is often characterized by continual self-correction (an arduous process!) suggests that learners are also inferring “when *should be* and *is* do not match” and “do[ing] something about the difference.” Through practice and feedback, skills such as these can become automatic [53]. Table IV presents recommendations from the literature relevant to developing learners’ situational awareness and offers corresponding examples in L2 learning settings.

TABLE IV. SITUATIONAL AWARENESS LINKS

Elements needed for situational awareness	**L2 learning content and practices that can be leveraged**
Observing, perceiving, and gathering information [24], [54], i.e., "track[ing] what is" [26]	• Directing attention to non-verbal cues when speaking with others • Noticing the time of day, etc. • Asking for information *Example: Teachers can help students observe and engage in multiple forms of information gathering, and point out that this is central to lessons about asking people's names, origins, feelings, identities, roles, nationalities, and ages, as well as lessons about places and customs.*
Seeking the meaning of gathered information [24], comparing observations of "what is" with one's knowledge of "what should be" [26] para. 9	• Inferring how someone is feeling • Evaluating trustworthiness • Checking for spelling errors *Example: One textbook activity [49, p. 25] required learners to infer how people in images were feeling (in order to project these people's likely responses to the question, "How's it going?").*
Projecting future status, predicting problems [24] (i.e., asking "How can 'x' fail?")	• Predicting conversation partners' behaviors in a given situation *Example: Teachers can encourage students to imagine themselves "staying with a host family…[and] ask how they think their French host father might react if they were to call him by his first name and why he would react that way" [49, p. 23]*

However, while multiple awareness-raising practices involving analysis, creativity, strategy, and context in L2 instruction are possible, the caveat is that implementation relies on the instructor's capacity "to recognise possibilities to generate discussion about language" [47, p. 60]. This invites an examination of how curricular materials and spaces might be explicitly developed to lift some of this burden off L2 instructors in fostering students' security mindsets.

B. Reimagining L2 learning curricular materials and spaces

We cannot expect all L2 instructors to be security experts with prior knowledge. In order to exploit links identified above, there would be a need to develop security-minded curricular resources that unpack these foundational links between language and security thinking for L2 instructors. Brief write-ups alongside course material could highlight various capabilities and concepts, explain their connection to security, and describe how they are fostered through given L2 skills or activities. Developmentally-appropriate explanations could also serve to help students identify areas of personal aptitude and interest. Moving beyond the identification and practice of foundational concepts, resources could be developed that leverage traditional L2 subject content to invite discussions about security topics. Content about phishing and pretexting could also be introduced through the deliberate selection of texts without compromising students' rich interaction with the target language. L2 content could be complemented and enriched by the inclusion of specific security-minded questions. This would likely be in beginners' first languages (L1); as students advance, it would increasingly be in the L2. (For educators who prefer not to use students' L1, I submit that alternative ways can be conceived for drawing attention to various security issues. Implementation is scalable and should be responsive to the goals and desires of the classroom.) Some examples are listed here:

- *Asking and telling names:* When is it okay to share a name? How can names be used to get your cooperation?
- *Greetings:* How might attention-getters (like *bonjour*) be used to impact situational awareness (positively and negatively)?
- *Numbers:* When is it more/less safe to share phone numbers? What can hackers do with it? What is the weakness of information encoded within numbers (lack of redundancy) and what precautions can be taken to make sure accurate data gets to the intended audience?
- *Interpreting photos/texts:* How can multiple data be used to address ambiguity? How could a strong desire to resolve ambiguity fail us?
- *Dialogue activities:* How does thinking someone is a friend/adversary impact what we will do or say?
- *Asking/telling personal information:* How many data points are necessary to identify an individual?
- *Interpreting and evaluating target-language content:* What information is available in this photo/text? How trustworthy is the image/text?

New lessons and spaces could also be created. L2 instructors often already display images of flags or café scenes; instructors could consider adding an (image of an) automatic bank machine or marketplace, setting the stage for students to engage in real-world target-language scenarios that introduce classmates playing the roles of strangers or potential adversaries. (In these instances, equipping students with optional vocabulary may be useful; when asking and telling time, for example, students might also find the phrase

"I'm sorry, I don't have my phone" quite useful – particularly if their dialogue scene has been set after dark by the bank machine.)

A panoply of avenues for potential exploitation suggest that L2 learning settings could prove effective resources for targeting the development of students' security mindsets. Moreover, many of these avenues align with calls in L2 instruction for more open-ended questions and interactive communication exchanges [55], and situated learning experiences that connect language with culture [56].

IV. SIGNIFICANCE

In what follows, I offer some preliminary thoughts regarding the value of implementation.

A. A novel conception for a novel population

These links between L2 learning and security thinking diverge from established conceptions of how language can support cybersecurity efforts. Traditionally, the link between language and security has been about the utility of a specific language (e.g., Urdu, Arabic, etc.) for carrying out security work. The advantages of fluency in particular languages are well documented within the general security sector [57], [58] and others have noted the prominent role that Linguistics plays in cybersecurity [59]. But such roles have still hinged on technical or highly specialized skills, leaving students in non-technical fields with few opportunities to get into cybersecurity [12]. However, in identifying a connection between security thinking and language learning in general, the door is opened for L2 classrooms potentially everywhere to participate.

The magnitude of this becomes clear when considering the most recent National K-12 Foreign Language Enrollment Survey Report [60]; almost 20% of K12 learners (or 10,638,282 students) in the U.S. educational system were enrolled in a FL program in 2017; that figure is much higher for the percentage of students participating in some form of high school FL study before graduation [61]. The number of children in ELL programs in the United States is estimated to be more than 10% or around 5 million students [61] and growing [62]. While FL and ELL populations are not mutually exclusive, these data nonetheless suggest a significant number of students in a position to meaningfully engage with fundamental security concepts. At least 23 U.S. states identify L2 study as a graduation requirement, while admission criteria at colleges and universities across the United States frequently require prior L2 study for matriculation [63]. For any of these students, L2 classrooms can serve as an gateway to technical, creative, and practical subfields within cybersecurity. While educational philosopher Nel Noddings [64, p. 675] wisely cautioned that we should be careful not to replace "systematic and sequential learning" with "incidental learning" – particularly for careers that demand exacting training – she affirmed that it could "be powerful in inspiring further study."

Casting the net wider could also serve to reduce cybersecurity workforce shortfalls while increasing diversity. Scholars have lamented the under-representation of women and minorities in cybersecurity, noting that teams made up of people with different backgrounds are more effective [65], [66]. Because the L2 content and processes examined here are already found in existing FL and ELL settings, and because implementation could be scaled to suit educational and institutional realities, this is an initiative that need not leave any districts or students behind.

B. The human factor

Rooting these efforts in L2 learning settings can reduce the risk of overlooking human factors. Just as language can and should be approached as more than "an abstract…set of rules…that exists independently of situated action in the world" [67, p. 2], so security can and should be, too. While both security and language can be viewed as a set of abstract technical principles, it is perhaps much easier in modern language settings to be reminded of the incompleteness of such a view. Thanks to language's profoundly technical and social aspects, security issues considered in this context can be both the object of intense analysis while remaining grounded in the human sphere.

Finally, I maintain that infusing L2 learning environments with security themes is not only beneficial for security thinking, but for L2 classes. As security themes deal with the whole of life, what it means to be human, and how to interact with others, L2 students have opportunities to consider questions of enduring import.

V. CONCLUSION

While scholars have debated whether security mindsets are taught or fostered, they have roundly acknowledged that greater development of security mindsets is needed [9], [3]. In this paper, I argued that K12+ L2 settings can be leveraged to foster situational awareness and analytical, creative, and practical fundamentals of security thinking in a wider population, potentially attracting more diverse talent into the field of cybersecurity. Without major curriculum overhaul, typical language concepts and topics in L2 learning settings can serve as in-roads for practicing security concepts. In tying abstract security principles to situations rooted in human communication, L2 learning is enriched; security mindsets come to life.

REFERENCES

[1] J. Hoag, "Evolution of a Cybersecurity Curriculum," in *Proceedings of the 2013 on InfoSecCD '13*. Accessed: Sep. 10, 2022. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2528908.2528925

[2] H. T. Le, "Meeting cybersecurity education challenges: A data analytics approach for continuous learning," Ph.D. Dissertation, George Mason University, Fairfax, VA, 2019. Accessed: Sep. 10, 2022. [Online]. Available: https://www.proquest.com/openview/5df3e1f6f61c9b68ec37afb7f2a1dcf7/1?cbl=18750&diss=y&pq-origsite=gscholar

[3] A. Siraj *et al.*, "Is there a security mindset and can it be taught?," in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, Virtual Event USA, Apr. 2021, pp. 335–336. doi: 10.1145/3422337.3450358.

[4] J. S. Jacob, "Towards a holistic interdisciplinary education in cybersecurity," M.S. thesis, The University of Houston-Clear Lake, 2018. Accessed: Sep. 11, 2022. [Online]. Available: https://uhcl-ir.tdl.org/handle/10657.1/1445

[5] W. H. Dutton, "Fostering a cyber security mindset," *Internet Policy Rev.*, vol. 6, no. 1, Jan. 2017, doi: 10.14763/2017.1.443.

[6] L. Hansen and H. Nissenbaum, "Digital disaster, cyber security, and the Copenhagen School," *Int. Stud. Q.*, vol. 53, no. 4, pp. 1155–1175, Dec. 2009, doi: 10.1111/j.1468-2478.2009.00572.x.

[7] S. T. Hamman and K. M. Hopkinson, "Teaching adversarial thinking for cybersecurity," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 4, no. 1, Art. no. 1, Oct. 2016.

[8] K. J. Knapp, C. Maurer, and M. Plachkinova, "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance," *J. Inf. Syst. Educ.*, vol. 28, no. 2, pp. 101–114, Dec. 2017.

[9] C. Severance, "Bruce Schneier: The Security Mindset," *Computer*, vol. 49, no. 2, pp. 7–8, Feb. 2016, doi: 10.1109/MC.2016.38.

[10] K. M. Carley, "Social cybersecurity: an emerging science," *Comput. Math. Organ. Theory*, vol. 26, no. 4, pp. 365–381, Dec. 2020, doi: 10.1007/s10588-020-09322-9.

[11] D. Morris, G. Madzudzo, and A. G. Perez, "Cybersecurity and the auto industry: the growing challenges presented by connected cars," *Int. J. Automot. Technol. Manag.*, vol. 18, no. 2, 2018, doi: 10.1504/IJATM.2018.092187.

[12] F. Sharevski, A. Trowbridge, and J. Westbrook, "Novel approach for cybersecurity workforce development: A course in secure design.," presented at the 2018 IEEE integrated STEM education conference (ISEC), Mar. 2018, pp. 175–180. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1806/1806.01198.pdf

[13] N. Young and S. Krishnamurthi, "Early post-secondary student performance of adversarial thinking," in *Proceedings of the 17th ACM Conference on International Computing Education Research*, Virtual Event USA, Aug. 2021, pp. 213–224. doi: 10.1145/3446871.3469743.

[14] V. Pournaghshband, "Teaching the security mindset to CS1 students," in *Proceeding of the 44th ACM technical symposium on Computer science education - SIGCSE '13*, Denver, Colorado, USA, 2013, p. 347. doi: 10.1145/2445196.2445299.

[15] A. H. Peterson, "Talk: Thinking like an attacker: Towards a definition and non-technical assessment of adversarial thinking, 12-1pm ET 4/30," *Department of Computer Science and Electrical Engineering*, Apr. 17, 2021. https://www.csee.umbc.edu/2021/04/talk-thinking-like-an-attacker-towards-a-definition-and-non-technical-assessment-of-adversarial-thinking-1-2pm-et-4-23/ (accessed Sep. 11, 2022).

[16] "Cyber Security Starts With Critical Thinking," *Insight Assessment*, Oct. 09, 2020. https://www.insightassessment.com/article/cyber-security-starts-with-critical-thinking (accessed Sep. 11, 2022).

[17] M. Padilla-Pagan Payano, "Situational awareness: A mindset, not a skill," *Dark Reading*, Oct. 10, 2019. https://www.linkedin.com/pulse/situational-awareness-mindset-skill-michael-padilla-pagan-payano (accessed Sep. 11, 2022).

[18] F. Katz, "Adversarial thinking: Teaching students to think like a hacker," in *KSU Proceedings on Cybersecurity Education, Research and Practice*, Kennesaw State University, Oct. 2019, vol. 1. [Online]. Available: https://digitalcommons.kennesaw.edu/ccerp/2019/education/1?utm_source=digitalcommons.kennesaw.edu%2Fccerp%2F2019%2Feducation%2 F1&utm_medium=PDF&utm_campaign=PDFCoverPages

[19] B. Schneier, "The security mindset: Schneier on security," *Schneier on Security*. https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html (accessed Sep. 11, 2022).

[20] T. Nassiokas, "The security mindset and the neurodiverse," *Genius Armoury*, Apr. 25, 2021. https://geniusarmoury.com/the-security-mindset-and-the-neurodiverse/ (accessed Sep. 11, 2022).

[21] J. Esteves, E. Ramalho, and G. De Haro, "To improve cybersecurity, think like a hacker," *MIT Sloan Manag. Rev.*, vol. 58, no. 3, pp. 71–77, Spring 2017.

[22] G. Vigna, "How to think like a hacker," *Dark Reading*, Oct. 10, 2019. https://www.darkreading.com/vulnerabilities-threats/how-to-think-like-a-hacker (accessed Sep. 11, 2022).

[23] R. Sternberg, *The triarchic mind*. New York: Penguin Books, 1988.

[24] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum. Factors*, vol. 37, no. 1, pp. 32–64, 1995, doi: 10.1518/001872095779049543.

[25] N. A. Stanton, P. R. G. Chambers, and J. Piggott, "Situational awareness and safety," *Saf. Sci.*, vol. 39, no. 3, pp. 189–204, Dec. 2001, doi: 10.1016/S0925-7535(01)00010-8.

[26] A. Horneman, "Situational awareness for cybersecurity: An introduction.," *SEI Blog*, Sep. 09, 2019. https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/ (accessed Apr. 10, 2022).

[27] Polaris Corporate Risk Management, "*Essential elements of a security mindset*." PDF document. Accessed: Sep. 10, 2022. [Online]. Available: https://polarisrsk.com/wp-content/uploads/2020/12/The-Essential-Elements-of-a-Security-Mindset.pdf

[28] M. Dark, "Thinking about cybersecurity," *IEEE Secur. Priv.*, vol. 13, no. 1, pp. 61–65, Feb. 2015, doi: 10.1109/MSP.2015.17.

[29] C. Servin, O. Kosheleva, and V. Kreinovich, "Adversarial Teaching Approach to Cybersecurity: A Mathematical Model Explains Why It Works Well," in 2020 *24th International Conference Information Visualisation (IV)*, Melbourne, Australia, Sep. 2020, pp. 313–316. doi: 10.1109/IV51561.2020.00058.

[30] E. Wegrzecka-Kowalewski, "Critical thinking in intensive language programs for international students in U.S. universities," Ph.D. Dissertation, University of Pittsburgh, Pennsylvania, United States, 2018. Accessed: Sep. 11, 2022. [Online]. Available: https://www.proquest.com/docview/2166850455/abstract/4E705F67109 84C9BPQ/1

[31] K. H. Pherson, "Key critical thinking skills for security professionals." https://www.securityinformed.com/insights/key-critical-thinking-skills-security-professionals-co-14642-ga.22310.html (accessed Sep. 11, 2022).

[32] Social-Engineer, "What is critical thinking?," *Security Boulevard*, Sep. 12, 2018. https://securityboulevard.com/2018/09/what-is-critical-thinking/ (accessed Sep. 11, 2022).

[33] R. B. Thorkelsdóttir, "Can critical thinking be taught? A Deweyan perspective on the notion of critical thinking applied to the Icelandic education," *J. Artist. Creat. Educ.*, vol. 12, no. 1, pp. 61–68, 2018.

[34] K. Bhandari, "Teaching language: Connecting content to context," *Azim Premji Univ. Learn. Curve*, pp. 40–43, Apr. 2020.

[35] D. Adger, *Language unlimited: The science behind our most creative power*. Oxford University Press, 2019.

[36] N. A. Charlow, "Practical language: Its meaning and use," Ph.D. Dissertation, University of Michigan, Michigan, United States, 2011. Accessed: Sep. 11, 2022. [Online]. Available: https://www.proquest.com/docview/918192562/abstract/EAB15E71D66F4F4DPQ/1

[37] William O'Grady, Michael Dobrovsky, and Francis Katamba, Eds., *Contemporary linguistics: An introduction*, 3rd ed. Harlow, United Kingdom: Pearson Longman, 1997.

[38] S. Krashen, "Second language acquisition.," *Second Lang. Learn.*, vol. 3, no. 7, pp. 19–39, 1981.

[39] C. E. Snow and M. Hoefnagel-Hoehle, *Age differences in second language acquisition*. 1975.

[40] R. J. Sternberg, "The theory of successful intelligence and its implications for language aptitude testing," in *Individual differences and instructed language learning*, vol. 2, P. Robinson, Ed. Amsterdam: John Benjamins, 2002, pp. 13–44.

[41] TechTarget Contributor, "What is disambiguation?: Definition from WhatIs.com," *TechTarget*. https://www.techtarget.com/searchdatamanagement/definition/disambiguation (accessed Sep. 11, 2022).

[42] R. H. Jones and J. C. Richards, *Creativity in language teaching: Perspectives from research and practice*. Routledge, 2015.

[43] P. Ricoeur, "Creativity in language," *Philos. Today*, vol. 17, no. 2, pp. 97–111, May 1973, doi: 10.5840/philtoday197317231.

[44] V. Agostini, I. Apperly, and A. Krott, “Early second language learning at school can boost creativity,” Jun. 2021.

[45] M. Dark and J. Mirkovic, “Evaluation theory and practice applied to cybersecurity education,” *IEEE Secur. Priv*., vol. 13, no. 2, pp. 75–80, Mar. 2015, doi: 10.1109/MSP.2015.27.

[46] P. Byrd, “What is pretexting? Tactics, techniques, and prevention,” *Hook Security Blog*, Feb. 28, 2022. https://hooksecurity.co/blog/pretexting (accessed Sep. 11, 2022).

[47] W. van der Hoek, W. Jamroga, and M. Wooldridge, “A logic for strategic reasoning,” in *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, New York, NY, USA, Jul. 2005, pp. 157–164. doi: 10.1145/1082473.1082497.

[48] Z. Dörnyei and R. Schmidt, *Motivation and second language acquisition*, vol. 2. Natl Foreign Lg Resource Ctr, 2001.

[49] Jean-Paul Valette and Rebecca Valette, *Discovering French today 1, 1a, 1b; Teacher’s edition*, 1st ed. Evanston, IL: Holt-McDougal, 2013.

[50] Robert Di Donato and Monica D. Clyde, *Deutsch: Na Klar!*, 8th ed. McGraw-Hill Education, 2020.

[51] P. Robinson, A. Mackey, S. Gass, and R. Schmidt, “Attention and awareness in second language acquisition,” in *The Routledge handbook of second language acquisition*, Routledge, 2013, pp. 247–267.

[52] “About: Association for Language Awareness.” https://www.languageawareness.org/?page_id=48 (accessed Sep. 12, 2022).

[53] D. Kahneman, *Thinking, fast and slow*. Macmillan, 2011.

[54] Eric S. Toner, “Creating situational awareness: A systems approach,” Institute of Medicine Forum on Medical and Public Health Preparedness for Catastrophic Events, Washington, DC, White paper, 2010. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK32848

[55] Yoones Tavoosy and Reza Jelvah, “Language teaching strategies and techniques used to support students learning in a language other than their mother tongue.,” *Int. J. Learn. Teach*., vol. 11, no. 2, pp. 077–088, 2019.

[56] Beatrice Dupuy and Kristen Michelson, “Introduction. Shifting paradigms: Reshaping discourse and practice for a more situated approach to second language education.,” in *Pathways to Paradigm Change: Critical Examinations of Prevailing Discourses and Ideologies in Second Language Education*, Beatrice Dupuy and Kristen Michelson, Eds. Boston: Cengage Thomson, 2019, pp. 1–8. [Online]. Available: https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/100b4046-ce84-4f34-bde6-93b15cbef15f/content

[57] C. King, “The decline of International Studies: Why flying blind is dangerous.,” *Foreign Aff*., vol. 94, no. 4, pp. 88–98, 2015.

[58] T. A. Taha, “Arabic as ‘a critical-need’ foreign language in post-9/11 era: A study of students’ attitudes and motivation,” *J. Instr. Psychol*., vol. 34, no. 3, pp. 150–160, Sep. 2007.

[59] J. L. Klavans, “Cybersecurity: What’s language got to do with it?,” Computational Linguistics and Information Processing (CLIP) Laboratory University of Maryland Institute for Advanced Computer Studies (UMIACS), White paper, 2015. [Online]. Available: https://drum.lib.umd.edu/bitstream/handle/1903/17165/LAMP-TR-158.pdf?sequence=1

[60] American Councils for International Education, “The national K-12 foreign language enrollment survey report,” The Language Flagship at the Defense Language and National Security Education Office, 2017. [Online]. Available: https://www.americancouncils.org/sites/default/files/FLE-report-June17.pdf

[61] C. De Brey, T. D. Snyder, A. Zhang, and S. A. Dillow, “Digest of education statistics 2019 (NCES 2021-009),” National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education, Washington, DC, Government report, 2021. [Online]. Available: https://files.eric.ed.gov/fulltext/ED611019.pdf

[62] “Our Nation’s English learners,” Our Nation’s English Learners. https://www2.ed.gov/datastory/el-characteristics/index.html (accessed Sep. 11, 2022).

[63] L. Jimenez and S. Sargrad, “Are high school diplomas really a ticket to college and work?,” *Wash. DC Cent. Am. Prog*., 2018, [Online]. Available: https://www.americanprogress.org/issues/education-k-12/reports/2018/04/02/447717/high-school-diplomas/

[64] N. Noddings, “Teaching themes of care,” *Phi Delta Kappan*, vol. 76, no. 9, pp. 675–679, May 1995.

[65] J. R. S. Blair, A. O. Hall, and E. Sobiesk, “Educating future multidisciplinary cybersecurity teams,” *Computer*, vol. 52, no. 3, pp. 58– 66, Mar. 2019, doi: 10.1109/MC.2018.2884190.

[66] D. N. Burrell and C. Nobles, “Recommendations to Develop and Hire More Highly Qualified Women and Minorities Cybersecurity Professionals,” in *International Conference on Cyber Warfare and Security*, Reading, United Kingdom, 2018, pp. 75–81. Accessed: Dec. 10, 2022. [Online]. Available: https://www.proquest.com/docview/2018924017/abstract/764C204985B C4EB9PQ/1

[67] B. H. Hodges, S. V. Steffensen, and J. E. Martin, “Caring, conversing, and realizing values: new directions in language studies,” *Lang. Sci*., vol. 34, no. 5, pp. 499–506, Sep. 2012, doi: 10.1016/j.langsci.2012.03.006.