ISSN: 2473-4901
v12 n6768

From Deficit to Design: Neuroinclusive Course Design in Online Cybersecurity Education

Anthony W. (Tony) Rose
roseaw@miamioh.edu
Miami University
Hamilton, OH, 45011, USA

Abstract

Online cybersecurity education is often described as flexible and accessible, yet course structures can unintentionally create barriers for neurodivergent learners, including autistic students. These barriers may not stem from cybersecurity concepts themselves but from unclear instructions, fragmented platforms, rigid deadlines, timed assessments, narrow expectations for participation, and hidden assumptions about executive functioning, communication, and prior technical experience. This conceptual paper argues that online cybersecurity courses should move beyond an accommodation-only approach toward neuroinclusive design that anticipates learner variability from the outset. Drawing on disability studies, disability justice, neurodiversity research in higher education, and Universal Design for Learning, the paper reframes neurodivergent students as expected and valued members of the cybersecurity learning community rather than as exceptions to an otherwise neutral course design. The paper proposes five design commitments for neuroinclusive online cybersecurity education: clarity before complexity, flexibility without lowering standards, multimodal access, authentic demonstration of skill, and belonging by design. These commitments are applied to common cybersecurity learning activities, including vulnerability scanning labs, log analysis exercises, incident response simulations, discussion boards, capture-the-flag activities, and group projects. The paper concludes that neuroinclusive design does not reduce rigor; rather, it better aligns cybersecurity instruction with the field's reasoning, documentation, collaboration, and problem-solving practices.

Keywords: cybersecurity education, neurodiversity, autism, online learning, Universal Design for Learning, accessibility

From Deficit to Design: Neuroinclusive Course Design in Online Cybersecurity Education

Anthony W. (Tony) Rose

1. INTRODUCTION

Cybersecurity education depends on learners developing complex forms of technical reasoning. Students are asked to interpret system behavior, identify patterns, detect anomalies, troubleshoot ambiguous situations, document evidence, and recommend appropriate action. These practices require persistence, attention to detail, systems thinking, and the ability to make sense of incomplete or evolving information. In this sense, cybersecurity is a field in which cognitive diversity should be viewed as an asset.

Yet online courses designed to prepare students for cybersecurity work may unintentionally privilege narrow assumptions about how successful learners communicate, manage time, process information, participate, and demonstrate competence. Online cybersecurity students often navigate learning management systems, virtual machines, cyber ranges, command-line tools, packet captures, scanners, discussion forums, documentation platforms, and collaborative workspaces. When these environments are not intentionally designed, students may encounter barriers unrelated to the cybersecurity learning objective. A student may understand vulnerability remediation but struggle to interpret a vague lab prompt. A student may be able to analyze logs but become overwhelmed by poorly sequenced instructions. A student may have strong technical reasoning but perform poorly on a timed quiz that primarily measures speed, anxiety tolerance, or familiarity with test formats.

These design issues are especially important for neurodivergent learners, including autistic students and those with ADHD, dyslexia, anxiety, executive-function differences, sensory-processing differences, and other forms of cognitive difference. Neurodivergent students are not a homogeneous group, and no single design approach will meet every need. However, research on neurodiversity in higher education emphasizes that student success is shaped not only by individual characteristics but also by institutional expectations, teaching practices, disclosure pressures, and whether learning environments communicate belonging (Clouder et al., 2020; Dwyer et al., 2023; Hamilton & Petty, 2023; Syharat et al., 2023).

This paper argues that online cybersecurity education should shift from a deficit-oriented or accommodation-only model to neuroinclusive design. Accommodation processes remain important and legally necessary, but they are not sufficient. An accommodation-only approach often leaves the original course design unexamined. The course is treated as neutral, and the student is expected to disclose, document, request, and justify support after barriers arise. For neurodivergent students, this can create additional emotional and cognitive labor. A design-oriented approach asks a different question: What barriers can be anticipated and reduced before students must request exceptions?

This paper offers a conceptual framework for designing neuroinclusive online cybersecurity courses. It first examines how deficit thinking and accommodation-only models can shape cybersecurity education. It then applies perspectives on disability, neurodiversity, and Universal Design for Learning to the online cybersecurity classroom. Finally, it proposes five design commitments that faculty can use to examine and redesign common cybersecurity learning activities while preserving authentic disciplinary challenge and technical rigor.

2. CONCEPTUAL APPROACH AND LITERATURE SYNTHESIS

This paper uses a conceptual synthesis rather than a systematic review or empirical research design. The literature was purposively organized across four intersecting areas relevant to the problem: neurodiversity in higher education and STEM (Clouder et al., 2020; Dwyer et al., 2023; Hamilton & Petty, 2023; Syharat et al., 2023), disability and justice-oriented approaches to inclusion (Annamma et al., 2013; Lin, 2022; Seale, 2023), online learning and cognitive load (Le Cunff et al., 2024a, 2024b,

2024c, 2025a; Tate & Warschauer, 2022), and inclusive computing and cybersecurity education (Garcia et al., 2023; Ismailov, 2022; Kävrestad et al., 2024; Zastudil et al., 2025). Sources were selected because they addressed learner variability, barriers created or amplified by educational environments, accessible course design, or the cognitive and instructional demands of computing and cybersecurity learning.

The synthesis was iterative. Recurring concerns across these literatures—including unclear or implicit expectations, extraneous cognitive demands, limited modes of participation or demonstration, disclosure-dependent support, and belonging—were considered in relation to common online cybersecurity activities. Overlapping principles were then consolidated into five design commitments: clarity before complexity, flexibility without lowering standards, multimodal access, authentic demonstration of skill, and belonging by design. The framework is therefore offered as a set of conceptually derived design commitments rather than as a set of empirically validated interventions.

A central challenge in disability and neurodiversity work in higher education is the tendency to locate difficulty primarily in the student. When a student struggles with an assignment, the explanation may be framed as a lack of motivation, independence, professionalism, or technical ability. This framing can obscure the role of course design. In online cybersecurity courses, barriers may be embedded in routine instructional practices: unclear lab instructions, hidden success criteria, rigid deadlines, unstructured group work, dense, text-heavy modules, inaccessible media, timed assessments, or discussion formats that define participation too narrowly.

The distinction between difficulty and barrier is important, but it is not always simple. Cybersecurity education should be challenging. Students need opportunities to troubleshoot, persist, reason through ambiguity, work with incomplete information, and make decisions under uncertainty. These demands may be authentic features of cybersecurity practice rather than barriers to be removed. At the same time, not all difficulty is educationally meaningful. If the goal of a lab is to analyze suspicious authentication logs, students should be challenged to identify evidence, compare normal and abnormal activity, explain their reasoning, and recommend action. They should not be primarily challenged by unclear file locations, missing examples, ambiguous submission expectations, or inaccessible instructions unless navigating those conditions is itself part of the stated learning outcome.

A deficit-oriented interpretation might view a student who struggles with a vague lab as lacking independence. A design-oriented interpretation asks whether the lab assumes prior knowledge, obscures essential steps, or fails to distinguish the cybersecurity challenge from the logistical work required to access it. A deficit-oriented interpretation might view a student who avoids discussion boards as disengaged. A design-oriented interpretation asks whether participation has been defined too narrowly. A deficit-oriented interpretation might view poor performance on a timed quiz as evidence of weak understanding. A design-oriented interpretation asks whether the assessment measures cybersecurity reasoning or merely processing speed.

Moving from deficit to design does not deny that students have different needs or that cybersecurity includes legitimate professional demands. Instead, it asks instructors to distinguish intentionally designed disciplinary challenge from incidental course difficulty. A useful decision test is whether the challenge is explicitly connected to a learning outcome, whether removing it would prevent students from practicing an authentic cybersecurity competency, whether it is introduced at an appropriate point in the curriculum, and whether performance on that challenge is represented in the assessment criteria. Ambiguity, time pressure, or independent troubleshooting may therefore be appropriate when they are part of what students are intended to learn. Disability and neurodiversity perspectives additionally encourage educators to examine how environments, expectations, tools, and institutional norms shape who can demonstrate competence.

4. NEURODIVERSITY AND CYBERSECURITY EDUCATION

Cybersecurity provides an important context for neuroinclusive design because the discipline itself depends on diverse ways of thinking. Security professionals examine logs, identify anomalies, trace patterns across systems, test assumptions, document evidence, and imagine how systems might fail or be exploited. These practices can align with the strengths of some neurodivergent learners. However, it is important not to stereotype autistic or neurodivergent students as naturally suited to cybersecurity.

Neurodivergent learners are diverse. Not all autistic students are interested in cybersecurity, and not all neurodivergent students share the same strengths, needs, or preferences.

The more important point is that cybersecurity education should recognize a broader range of cognitive approaches as legitimate. A student may demonstrate engagement through a carefully documented script, a precise explanation of a vulnerability, a threat model diagram, a packet analysis, or a structured incident timeline. Engagement does not always look like verbal fluency, rapid posting, spontaneous collaboration, or public confidence. Technical competence does not always look like speed. Professionalism does not always look like ease in the face of ambiguous social expectations.

Online cybersecurity courses can unintentionally create barriers because they often require students to navigate multiple layers of complexity at once. A single lab may require students to understand cybersecurity concepts, configure a virtual environment, interpret tool output, troubleshoot errors, capture evidence, write a report, and submit artifacts in a specific format. For some students, especially neurodivergent students, the cumulative executive-function demands of these tasks may become the primary challenge. When this happens, assessment may no longer cleanly measure the intended cybersecurity outcome.

Research on neurodiversity and cognitive load in online learning suggests that digital learning environments can increase extraneous cognitive load when course organization, communication, and platform structures are not intentionally designed (Le Cunff et al., 2024a, 2024b, 2024c, 2025a). Computing-education and cybersecurity-training scholarship likewise provides a basis for examining inclusion and cognitive accessibility within technical instruction (Garcia et al., 2023; Kävrestad et al., 2024; Zastudil et al., 2025). In cybersecurity education, unnecessary load may stem from unclear instructions, fragmented platforms, or hidden assumptions about prior technical experience. Neuroinclusive design asks faculty to distinguish that instructional complexity from the essential complexity of cybersecurity itself.

5. UNIVERSAL DESIGN FOR LEARNING AS PRACTICE

Universal Design for Learning (UDL) offers a practical way to translate neuroinclusive commitments into course design. UDL assumes that learner variability is normal. Students differ in how they engage with learning, access information, and demonstrate understanding. Therefore, courses can provide multiple pathways where those pathways remain aligned with the intended learning outcome. Inclusive design research in computing education similarly suggests that accessibility and inclusion can be integrated into regular computing instruction rather than treated as separate or remedial concerns (Garcia et al., 2023; Ismailov, 2022).

In online cybersecurity courses, multiple means of engagement might include letting students choose among scenarios, roles, or challenge pathways. For example, in an incident response unit, students might work as log analysts, threat researchers, remediation planners, or technical writers. Multiple means of representation might include text instructions, short videos, diagrams, annotated screenshots, sample command outputs, glossaries, and walkthroughs. Multiple means of action and expression might include written reports, screencasts, diagrams, scripts, annotated evidence, oral walkthroughs, or incident response briefs.

A justice-oriented use of UDL does not mean lowering expectations. This distinction is essential in cybersecurity education, where rigor and professional competence are paramount. Neuroinclusive design does not reduce the complexity of cybersecurity concepts. Instead, it reduces barriers that are not central to the learning objective. If the learning objective is vulnerability analysis, students should be assessed on their ability to interpret results, prioritize risk, justify decisions, and recommend remediation. They should not be unintentionally assessed on their ability to guess what the instructor wanted in a screenshot or to infer unstated formatting rules.

UDL also helps distinguish between flexibility and a lack of structure. Neuroinclusive design is not simply giving students unlimited options without guidance. In many cases, clear structure, predictable expectations, and transparent criteria can support access to the intended learning. However, the cybersecurity context places an important boundary on this principle: ambiguity, unfamiliar tools, incomplete information, rapid prioritization, and independent troubleshooting may themselves be

competencies. The contribution of the present framework is therefore not to replace UDL, disability justice, or inclusive computing guidance, but to translate them into a discipline in which educators must deliberately decide which uncertainty should be clarified and which uncertainty should be preserved for authentic practice.

6. FIVE DESIGN COMMITMENTS

This paper proposes five design commitments for neuroinclusive online cybersecurity education: clarity before complexity, flexibility without lowering standards, multimodal access, authentic demonstration of skill, and belonging by design. These commitments translate perspectives on disability, neurodiversity, UDL, and inclusive computing into course-level decisions for cybersecurity faculty. They are not prescriptions for maximizing structure or choice. Additional formats, examples, scaffolds, and assessment pathways can increase instructor workload, course-maintenance demands, grading complexity, and even student choice load. Excessive scaffolding may also diminish discovery or independence. The goal is purposeful alignment among the learning outcome, the source of difficulty, the support provided, and the evidence students are expected to produce.

6.1 Clarity Before Complexity

Clarity before complexity means that students should understand an activity's purpose, tools, deliverables, and success criteria before being asked to navigate complex technical tasks, except where discovering those elements is itself part of the learning objective. Cybersecurity learning often involves ambiguity, but the ambiguity should be intentional. A vulnerability scanning lab might include a setup checklist, target description, sample finding, glossary, and report template when setup and reporting conventions are not being assessed. In a more advanced activity, however, selecting tools or determining an investigation path may appropriately remain open-ended.

6.2 Flexibility Without Lowering Standards

Flexibility without lowering standards means students may have multiple pathways to demonstrate the same rigorous learning outcome when the format itself is not a competency. A student might submit a written report, annotated evidence, a screencast walkthrough, or a structured incident brief while still being required to provide evidence, explain reasoning, and connect findings to appropriate technical action. Conversely, a standardized written or oral format may be appropriate when professional communication in that format is explicitly being assessed. Flexibility is therefore bounded by the learning outcome rather than treated as an end in itself.

6.3 Multimodal Access

Multimodal access means key course information can be made available in more than one usable form when doing so supports access to the same learning goal. Cybersecurity instruction often relies on dense text, command-line demonstrations, screenshots, and tool output. Short videos, transcripts, diagrams, annotated examples, checklists, and downloadable references may help students process that information. These supports need not duplicate every resource in every possible format; instructors can prioritize high-barrier materials and formats that are sustainable to create and maintain.

6.4 Authentic Demonstration of Skill

An authentic demonstration of skill means assessments should measure the cybersecurity competency they claim to measure. Timed quizzes, standardized reports, rigid submission formats, and speed-based exercises may be useful when rapid recognition, prioritization, or a particular professional communication form is part of the stated outcome. They should be used more cautiously when they function only as proxies for technical competence. In an incident response simulation, for example, students might construct a timeline, identify indicators of compromise, justify containment steps, and produce an executive summary. In a capture-the-flag activity, process documentation and explanations of failed attempts may provide evidence of learning alongside flags captured.

6.5 Belonging By Design

Belonging by design means that courses should make clear from the start that cognitive diversity is expected and valued. This can be done through syllabus language, course orientation materials, communication norms, flexible participation structures, and examples that present different ways of thinking as legitimate. In cybersecurity education, belonging also means recognizing that the field depends on teams, documentation, peer review, playbooks, and collaborative problem-solving. Courses should not overemphasize unsupported independence when the profession itself relies on structured interdependence. A student who uses a checklist, template, peer feedback process, or troubleshooting guide is no less professional. They are using tools similar to those used in technical workplaces.

7. APPLICATIONS TO CYBERSECURITY LEARNING ACTIVITIES

The five design commitments can be applied to common cybersecurity learning activities. Table 1 summarizes predictable barriers and possible neuroinclusive design responses. These strategies are proposed practices rather than evaluated interventions, and their appropriateness depends on the course level, learning outcome, available resources, and professional competencies being developed. The goal is not to remove challenge but to align challenge more deliberately with the intended cybersecurity outcome.

Activity	Potential Barrier	Neuroinclusive Redesign Strategy
Vulnerability scanning lab	Students may be assessed on tool setup, screenshot hunting, or guessing report expectations rather than vulnerability interpretation.	When setup/reporting are not outcomes, consider a setup checklist, expected outputs, sample finding, severity guide, report template, and rubric focused on interpretation and remediation.
Log analysis exercise	Large unstructured files and unfamiliar fields can overwhelm students before they reach the analytical task.	Consider a scenario overview, field glossary, examples, guiding questions, or checkpoints; fade these supports when independent analysis becomes the intended competency.
Incident response simulation	Evidence volume, ambiguity, and unclear roles can create extraneous cognitive load and social barriers.	Consider staged evidence, an investigation playbook, defined team roles, or multiple submission formats; retain uncertainty or time pressure when those are explicitly assessed competencies.
Capture-the-flag activity	Scoreboards may reward speed, prior experience, and comfort with ambiguity more than learning process.	Consider tiered hints, process credit, reflection, and varied participation; retain speed-based scoring when rapid problem solving is an explicit objective.
Online discussion	Required post-and-reply formats may define participation too narrowly.	Allow text, audio, video, diagrams, annotated artifacts, or role-based responses such as analyst, defender, auditor, attacker, or policy advisor.
Group cybersecurity project	Undefined roles, timelines, and communication expectations can obscure technical learning.	Define roles, milestones, communication norms, peer review points, and options for asynchronous collaboration.

Table 1. Common Online Cybersecurity Barriers and Neuroinclusive Redesign Strategies

7.1 Vulnerability Scanning Labs

Traditional vulnerability scanning labs may ask students to run a scanner, interpret results, and submit screenshots or a report. A proposed neuroinclusive redesign might clarify setup, expected evidence, and reporting criteria when those elements are not the learning target. In a more advanced course, however, tool selection, troubleshooting, or determining an appropriate reporting structure may themselves be competencies and should not automatically be scaffolded away.

7.2 Log Analysis Exercises

A traditional log analysis activity may involve providing a large file and asking students to identify suspicious behavior. A proposed redesign might initially include a scenario overview, field glossary, examples, checkpoints, and guiding questions. Those supports can be reduced over time when independently determining what matters in an unfamiliar dataset becomes part of the intended competency.

7.3 Incident Response Simulations

Incident response simulations are appropriately demanding because students must process evidence, manage uncertainty, and make decisions. A proposed neuroinclusive version might stage evidence, define team roles, or provide an investigation playbook when the primary focus is evidence interpretation and response planning. More advanced simulations may intentionally introduce simultaneous information, uncertain roles, or time pressure when coordination and prioritization under pressure are explicitly assessed.

7.4 Capture-the-Flag Activities

Capture-the-flag activities may reward speed, prior experience, and comfort with ambiguity in addition to the intended technical skill. A proposed neuroinclusive CTF might include tiered hints, process credit, reflection prompts, or individual and collaborative pathways when the primary goal is skill development. Competitive speed-based scoring can still be appropriate when rapid problem solving is an explicit objective and the scoring system is interpreted accordingly.

7.5 Online Discussions and Group Projects

The common "post once, reply twice" model may define participation more narrowly than the learning objective requires. Proposed alternatives could include text, audio, video, diagrams, annotated artifacts, or role-based prompts when the goal is analysis or communication rather than mastery of a specific medium. Group projects may likewise benefit from defined roles, milestones, communication norms, and asynchronous options, while still preserving authentic collaboration demands when teamwork itself is being assessed.

8. IMPLICATIONS FOR FACULTY AND PROGRAMS

For faculty, neuroinclusive design begins with a shift in diagnostic questions. Rather than asking only why a student struggled, instructors can ask what the design required the student to manage. Did the activity assess the intended learning outcome? Were instructions explicit? Were examples provided? Were students offered multiple ways to access information and demonstrate understanding? Did the course reward speed or confidence more than reasoning? Did participation structures recognize different forms of engagement?

Faculty do not need to redesign an entire course at once. Neuroinclusive redesign can begin with high-barrier assignments, but implementation has real costs. Revising labs, creating additional formats, maintaining examples, and calibrating multiple assessment pathways require time and institutional support. Faculty can therefore prioritize changes where incidental course difficulty is most likely to interfere with the stated learning outcome, and programs can support that work through shared templates, instructional-design assistance, and professional development.

At the program level, neuroinclusive cybersecurity education should not rely solely on individual faculty interest. Programs can assess whether course sequences, lab platforms, assessment practices, and advising structures accommodate learner variability. Institutions can support faculty through professional development, accessible course templates, instructional design support, and mechanisms for hearing neurodivergent students' experiences. Participatory approaches to neurodiversity research underscore the importance of listening to neurodivergent students when identifying barriers and design priorities (Le Cunff et al., 2025b).

This work is especially important for cybersecurity pathways because the field continues to seek broader participation. If cybersecurity education aims to attract and retain diverse learners, it must examine not only recruitment but also course design. Access to a program is not the same as belonging within it. Neuroinclusive design can help ensure that students are not filtered out by avoidable barriers unrelated to cybersecurity competence.

9. LIMITATIONS AND FUTURE WORK

This paper is conceptual and pedagogical rather than empirical. It does not present student outcome data, survey results, or an evaluated intervention. Its contribution is to synthesize existing literature for the specific context of online cybersecurity education and translate that synthesis into proposed design commitments. The framework therefore should be treated as a set of design hypotheses and decision principles whose effectiveness, feasibility, and unintended consequences require empirical study.

Future work should examine how neurodivergent students experience specific structures in online cybersecurity courses and should include neurodivergent students in identifying priorities, co-designing changes, and interpreting results (Le Cunff et al., 2025b). Evaluation could combine implementation evidence with measures of belonging, perceived cognitive load, persistence, course completion, and cybersecurity performance. Studies should also examine instructor workload, sustainability, grading consistency, and possible unintended effects such as choice overload, over-scaffolding, or reduced opportunities for independence. Comparative work could test when supports should be provided, faded, or withheld as ambiguity, speed, and independent troubleshooting become explicit learning outcomes.

10. CONCLUSIONS

Online cybersecurity education can expand access to technical learning, but flexibility is not automatic. Online courses can either reduce barriers or reproduce them in digital form. For neurodivergent learners, including autistic students, barriers may include unclear instructions, fragmented platforms, rigid timelines, narrow participation expectations, inaccessible materials, and assessments that prioritize speed or compliance over cybersecurity reasoning.

This paper argues for a shift from deficit to design. Rather than treating neurodivergent students as exceptions who must request support only after barriers arise, cybersecurity educators can examine course structures in anticipation of learner variability. The five commitments proposed here—clarity before complexity, flexibility without lowering standards, multimodal access, authentic demonstration of skill, and belonging by design—are intended as design principles to be tested and refined, not as empirically established interventions.

Neuroinclusive cybersecurity education is not about making courses easier or eliminating uncertainty. It is about making instructional choices more deliberate: preserving ambiguity, time pressure, independent troubleshooting, and other forms of difficulty when they represent authentic cybersecurity competencies, while reducing complexity that is incidental to those competencies. Future implementation and research, especially with neurodivergent student input, will be necessary to determine where particular forms of structure, flexibility, and challenge best support learning, belonging, and professional preparation.

10. REFERENCES

Annamma, S. A., Connor, D., & Ferri, B. (2013). Dis/ability critical race studies (DisCrit): Theorizing at the intersections of race and dis/ability. Race Ethnicity and Education, 16(1), 1–31. https://doi.org/10.1080/13613324.2012.730511

Clouder, L., Karakus, M., Cinotti, A., Ferreyra, M. V., Fierros, G. A., & Rojo, P. (2020). Neurodiversity in higher education: A narrative synthesis. Higher Education, 80(4), 757–778. https://doi.org/10.1007/s10734-020-00513-6

Dwyer, P., Mineo, E., Mifsud, K., Lindholm, C., Gurba, A., & Waisman, T. C. (2023). Building neurodiversity-inclusive postsecondary campuses: Recommendations for leaders in higher education. Autism in Adulthood, 5(1), 1–14. https://doi.org/10.1089/aut.2021.0042

Garcia, R., Morreale, P., Letaw, L., Chatterjee, A., Patel, P., Yang, S., Escobar, I. T., Noa, G. J., & Burnett, M. (2023). "Regular" CS × inclusive design = smarter students and greater diversity. ACM Transactions on Computing Education, 23(3), 1–35. https://doi.org/10.1145/3603535

Hamilton, L. G., & Petty, S. (2023). Compassionate pedagogy for neurodiversity in higher education: A conceptual analysis. Frontiers in Psychology, 14, Article 1093290. https://doi.org/10.3389/fpsyg.2023.1093290

Ismailov, M. (2022). Catering to inclusion and diversity with universal design: A mixed-method study. Frontiers in Psychology, 13, Article 819884. https://doi.org/10.3389/fpsyg.2022.819884

Kävrestad, J., Rambusch, J., & Nohlberg, M. (2024). Design principles for cognitively accessible cybersecurity training. Computers & Security, 137, Article 103630. https://doi.org/10.1016/j.cose.2023.103630

Le Cunff, A.-L., Giampietro, V., & Dommett, E. (2024a). Neurodiversity and cognitive load in online learning: A focus group study. PLOS ONE, 19(4), Article e0301932. https://doi.org/10.1371/journal.pone.0301932

Le Cunff, A.-L., Giampietro, V., & Dommett, E. (2024b). Neurodiversity and cognitive load in online learning: A systematic review with narrative synthesis. Educational Research Review, 43, Article 100604. https://doi.org/10.1016/j.edurev.2024.100604

Le Cunff, A.-L., Giampietro, V., & Dommett, E. (2024c). Neurodiversity positively predicts perceived extraneous load in online learning: A quantitative research study. Education Sciences, 14(5), Article 516. https://doi.org/10.3390/educsci14050516

Le Cunff, A.-L., Martis, B.-L., Glover, C., Ahmed, E., Ford, R., Giampietro, V., & Dommett, E. J. (2025a). Cognitive load and neurodiversity in online education: A preliminary framework for educational research and policy. Frontiers in Education, 9, Article 1437673. https://doi.org/10.3389/feduc.2024.1437673

Le Cunff, A.-L., Ross, F., Westwood, S. J., Koya, S., Caldwell, D. M., Russell, A. E., & Dommett, E. J. (2025b). Key research questions to support neurodiversity in higher education: A participatory priority setting exercise. Education Sciences, 15(7), Article 839. https://doi.org/10.3390/educsci15070839

Lin, K. (2022). CS education for the socially-just worlds we need: The case for justice-centered approaches to CS in higher education. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education (pp. 265–271). https://doi.org/10.1145/3478431.3499291

Seale, J. (2023). Reimagining disability for the digital age: Why more than human-computer interaction is needed to ensure disabled university students' inclusion. Studies in Higher Education, 48(7), 1031–1044. https://doi.org/10.1080/03075079.2022.2135102

Syharat, C. M., Hain, A., Zaghi, A. E., Gabriel, R., & Berdanier, C. G. P. (2023). Experiences of neurodivergent students in graduate STEM programs. Frontiers in Psychology, 14, Article 1149068. https://doi.org/10.3389/fpsyg.2023.1149068

Tate, T., & Warschauer, M. (2022). Equity in online learning. Educational Psychologist, 57(3), 192–206. https://doi.org/10.1080/00461520.2022.2062597

Zastudil, C., IV, D. H. S., Tohamy, Y., Nasimova, R., Montross, G., & MacNeil, S. (2025). Neurodiversity in computing education research: A systematic literature review. In Proceedings of the 30th ACM Conference on Innovation and Technology in Computer Science Education V. 1 (pp. 114–120). https://doi.org/10.1145/3724363.3729088

APPENDIX A

Neuroinclusive Online Cybersecurity Course Design Checklist

Clarity before complexity

☐ Does each lab state its purpose, tools, steps, deliverables, and success criteria?
☐ Are examples, templates, or expected outputs provided when they do not compromise the learning goal?
☐ Is ambiguity intentionally tied to the cybersecurity outcome rather than created by missing instructions?

Flexibility without lowering standards

☐ Can students demonstrate the same outcome through more than one format?
☐ Does the rubric identify the required evidence, reasoning, and technical performance?
☐ Are deadlines and revision opportunities structured to support learning without removing accountability?

Multimodal access

☐ Are key instructions available in text and another format such as video, diagram, or annotated screenshot?
☐ Are videos captioned or paired with transcripts?
☐ Are command outputs, screenshots, and tools explained with readable labels or notes?

Authentic demonstration of skill

☐ Do assessments measure cybersecurity reasoning rather than speed alone?
☐ Can students receive credit for process documentation, troubleshooting, and justification?
☐ Are timed assessments used only when speed is part of the stated learning objective?

Belonging by design

☐ Does the syllabus communicate that learner variability is expected?
☐ Are participation options broader than one required discussion format?
☐ Are collaboration roles, communication expectations, and milestones clearly defined?