THE CYBER DEFENSE REVIEW
YEAR, VOL. XX, NO. XX, 1-12
https://doi.org/10.55682/cdr/XXXX-XXXX

RESEARCH ARTICLE

Insert The Title of Your Paper Here

First A. Author*[1,2], Second B. Author[1,3], Third C. Author[1]

[1]Army Cyber Institute, West Point, NY, USA
[2]Institution Two, City, State, Country
[3]Institution Three, City, Country

Sample text inserted for demonstration. Insert your abstract here, with no distinctive header. The abstract should be between 150 and 200 words. It should not contain bibliographical references. Your abstract must give readers a brief summary of your article. It should be informative and accessible: indicate the general scope of the article and state the main results obtained and conclusions drawn. The abstract must be complete in itself: it must not contain undefined abbreviations and must not refer to any table, figure, reference or equation numbers. The review process for research articles is double-blind: the submitted document should not include author information and should not include acknowledgments, or mentions (e.g., in citations or discussion of related work) that would make the authorship apparent. Upon acceptance, the author and affiliation information will be added to your paper.

Keywords: Insert 3-5 comma delimited keywords, keyword 2, keyword 3, keyword 4

* Corresponding author: first.author@example.org

ABOUT THIS TEMPLATE

The Cyber Defense Review manuscript template enables authors to type their content into the pre-existing set of paragraph formatting styles applied to the sample placeholder text. Throughout the document, you will find further formatting instructions and a summary of the information contained in the Instructions to Authors on the Cyber Defense Review website (https://cyberdefensereview.army.mil/).

In addition, some sections include guidance on academic writing; these are for inspiration purposes and are not prescriptive.

Manuscript Submission

Manuscripts must be submitted in Microsoft Word (.docx) format or as a LaTeX document (with all source files and compiled PDF) through the journal's online submission system (http://www.editorialmanager.com/cyberdefreview/default.aspx).

Submissions should be in English and written in a clear, concise, and scholarly tone. Use American English spelling and conventions throughout. Avoid jargon when possible and define acronyms upon first use.

Selecting your Submission Type

Research Articles. are peer-reviewed contributions presenting original, rigorous and theoretically grounded scholarship relevant to the cyber defense landscape. Given the multidisciplinary nature of the journal and its broad readership, including practitioners, academics, policymakers, and military professionals, we welcome a wide range of methodologically sound research approaches and submissions, from shorter analytical pieces to longer, in-depth studies. Typical length ranges from 3,000 to 10,000 words (excluding abstract and references), with shorter pieces expected to have a tightly scoped contribution and longer ones offering more substantial or integrative insights. Authors should ensure that their articles can be read at both interdisciplinary and disciplinary levels. **Every research article must clearly articulate its research question(s), contribution statement, describe the research design or methodology employed, and demonstrate engagement with existing academic literature.** Submissions should contribute to knowledge development through systematic analysis, empirical evidence, or theoretical advancement, rather than personal reflection or commentary.

Professional Commentaries. provide timely, practice-oriented reflections on current developments, operational challenges, or policy issues in the cyber defense landscape. These contributions are designed to stimulate informed discussion and share wisdom and knowledge across sectors. They do not require a formal research design or empirical data, but the strongest commentaries engage thoughtfully with relevant literature, frameworks, or debates

to support and enrich the author's argument or perspective. They are typically 2,500 to 6,000 words (excluding abstract and references) and written in an accessible tone. Submissions to the Professional Commentary track follow a single-blind review process, where the reviewers know the identity of the authors.

Responsible Use of Large Language Models and Generative AI Tools

We allow, and even encourage, authors to use Large Language Models (LLMs) and generative AI tools (e.g., ChatGPT, Gemini) to assist with writing, editing, or translation. Authors may use AI tools to enhance grammar, clarity, or spelling, without needing disclosure.

However, any use beyond basic language polishing must be done under the following three conditions and be transparently reported. First, all content produced must be correct, original, and accurately reflect the author's own intellectual contributions. Authors remain fully responsible for AI outputs as well as the appropriateness of the research process for which AI is used. Second, authors must clearly disclose any use of AI software when it generates substantive new text, code, tables, or figures. Such disclosures, detailing the tool used and sections affected (prompt text disclosure is left at the discretion of the authors), should be included in acknowledgements or appendices, with the level of detail matching the extent of AI use. Third, AI tools must never be listed as co authors; all listed authors must meet standard authorship criteria and are fully accountable for the content.

Copyright and Use of Third-Party Material

The author is responsible for securing permission for any copyrighted material included in the submission. The author must ensure the content of the submission does not contain material that is libelous or would violate copyright or otherwise infringe upon the rights of others, including patent, trademark, trade secret, or rights of privacy or publicity. Prior to publication of the article, the author shall provide the CDR with proof of consent to use all copyright-protected material.

If your paper contains material for which you do not have Open Access re-use permissions, please state this clearly by supplying the following credit line alongside the material: *Title of content, Author, Original publication, year of original publication, by permission of [rights holder]. This image/content is not covered by the terms of the Creative Commons licence of this publication. For permission to reuse, please contact the rights holder*.

Citing Related Work

The CDR uses a Chicago Manual of Style Author-Date citation style:
www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

In-text citations. : Sources are cited in the text, usually in parentheses, by the author's last (family) name and the publication year of the work cited. Author-date citations are usually placed just before a mark of punctuation. You can use the following commands:

Command	Output example	Description
`\autocite{HarknettSmeets2020}`	(Harknett and Smeets 2020)	Parenthetical citation, typically used at the end of a sentence.
`\textcite{HarknettSmeets2020}`	Harknett and Smeets (2020)	In-text citation that integrates the author's name into the sentence.
`\gentextcite{Sanger2018}`	Sanger's (2018)	Genitive (possessive) in-text citation.
`\autocite[15]{Sanger2018}`	(Sanger 2018, 15-16)	Adds a specific page number or page range to the citation.
`\autocite[comment]{Dawson2023}`	(Dawson 2023, comment)	Adds a short comment. Can be combined with page number.

Table 1. Quick reference for common Chicago-style citation commands in the CDR template.

Where the author's name appears in the text, it need not be repeated in the parenthetical citation. For example: Sanger's (2018) book on the cyber age warns against…"

When the same page or pages in the same source are cited more than once in one paragraph, the parenthetical citation can be placed after the last reference or at the end of the paragraph.

When a reference list includes two or more works published in the same year by the same author or authors, the text citations as well as the reference list must use the letters a, b, and so on. For example: GAO (2020a, 2020b). This will be done automatically if you use the built in citation commands.

For works by two or three authors, all names are included (Sánchez Chamorro, Toebosch, and Lallemand 2024). For more than three authors, only the name of the first author is used, followed by 'et al.' (Distler et al. 2021). This will be done automatically if you use the citations command.

Consult the References section at the end of this document for instructions on how sources in the reference list should appear. Please ensure that your bibtex entries are accurate, particularly when it comes to government documents (directives, doctrines, field manuals, military regulations, reports, and strategy documents). For example: (U.S. Department of Defense 2018)

THIS IS AN EXAMPLE FOR FIRST LEVEL HEAD – SECTION HEAD

This is an Example for Second Level Head – Subsection Head

This is an Example for Third Level Head – Subsubsection Head. Sample text inserted for demonstration. Organize the main text of your article using section headings and subheadings (this template supports three levels: section, subsection, and subsubsection).

Figures and Tables

Figures and tables should be clearly labeled and embedded within the main text near their first mention. Include descriptive captions and cite all figures/tables in the body of the manuscript. Ensure all visuals are high-resolution (minimum 300 dpi) and suitable for grayscale printing. Please submit any tables in your main article document in an editable format (Word or TeX/LaTeX, as appropriate), and not as images.

Authors are encouraged to follow accessibility best practices when preparing visuals:

- Provide alt text for all figures and tables to describe their content for screen readers.
- Use symbols, patterns, or labels in graphs and charts instead of color alone, as all papers are printed in grayscale. Color should not be used to convey meaning, since it will not appear in the print version.
- Use clear, legible fonts and ensure high contrast between text and background.

Figures. The "`figure`" environment should be used for figures. One or more images can be placed within a figure. If your figure contains third-party material, you must clearly identify it as such, as shown in Figure 1 below. Your figures should contain a caption that describes the figure to the reader. Figure captions are placed *below* the figure.

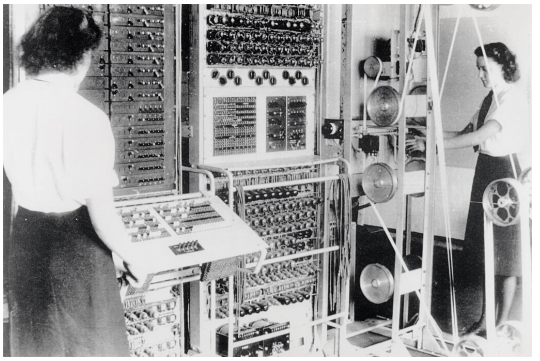

Figure 1. A Colossus Mark 2 codebreaking computer being operated by Dorothy Du Boisson (left) and Elsie Booker (right), 1943. Unknown author, via Wikimedia Commons. (https://commons.wikimedia.org/wiki/File:Colossus.jpg).

Every figure should also have a description unless it is purely decorative. These descriptions convey what is in the image to someone who cannot see it. They are also used by search engine crawlers for indexing images, and when images cannot be loaded. A figure description

must be plain text less than 2000 characters long (including spaces). Figure descriptions should not repeat the figure caption – their purpose is to capture important information that is not already provided in the caption or the main text of the paper.

Tables. The "`cdrart`" document class includes the "`booktabs`" package (https://ctan.org/pkg/booktabs) for preparing high-quality tables. The contents of the table must go in the **tabular** environment, to be aligned properly in rows and columns, with the desired horizontal and vertical rules. Detailed instructions on **tabular** material are found in the *LaTeX User's Guide*. To set a table that takes up the whole width of the page, use the environment **table*** to enclose the table's contents and the table caption. As with a single-column table, this wide table will "float" to a location deemed more desirable. Always use midrule to separate table header rows from data rows, and use it only for this purpose. This enables assistive technologies to recognize table headers and support their users in navigating tables more easily. Following this sentence is the point at which Table 2 is included in the input file.

Non-English or Math	Frequency	Comments
Ø	1 in 1,000	For Swedish names
π	1 in 5	Common in math
$	4 in 5	Used in business
Ψ_1^2	1 in 40,000	Unexplained usage

Table 2. Frequency of Special Characters

Special Formatting

Verbatim Quotes. You can include verbatim quotes within your text by enclosing them in quotation marks. For quotes longer than three lines, format them as a block quote, for example:

> Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna.

You can also use italics when introducing a new key term (e.g., cyber health security theory), and bold for emphasis if needed. Example: "We define *cyber health security theory* as…"

Footnotes. Footnotes may be used only for explanatory comments, not for bibliographic references. Footnotes can be added using the command `\footnote`. Here is a footnote [1]

1. Here is a footnote

RESEARCH ARTICLE RECOMMENDATIONS

1 INTRODUCTION

[The introduction should briefly place the study in context and highlight why it is important. Define the purpose of the work and its significance. Suggested guiding questions:

- What is the problem or opportunity? Who is impacted, and in what context? Why do we need to address it?
- Why does it matter now? How significant is the issue (use evidence such as reports, survey data, or prior research)?
- What did you do to address it (summarize in 3 sentences)?
- What is your contribution and who benefits from it?
- What are the key concepts of your paper, and how do you define them (Definitions can also be provided in the Related Work section if more appropriate.)

Organize from general to specific. Do not include results or discussion here. Add references to literature or data that scope the problem and make the case for timeliness.]

2 BACKGROUND

[Provide additional historical, technical, or conceptual background if needed. This section is optional and may be merged into the introduction if concise.]

3 RELATED WORK

[Discuss prior work and situate your study in the body of academic and professional literature. Do not simply list sources; synthesize and analyze. Address:

- How have others tried to solve this problem?
- What are the strengths and shortcomings of prior approaches?
- What opportunities remain for your work to address?

Clearly define key concepts that are used throughout the paper (if not already done in the introduction). We recommend dividing this section into subsections with meaningful titles.]

4 RESEARCH DESIGN

[Describe the methodology clearly and in enough detail for others to evaluate or replicate. Depending on your discipline and study type, include:

- Research objectives (sometimes includes precise research questions or hypotheses)
- Study design (e.g., case study, experiment, literature review, survey, simulations, mixed-methods approaches)

- Participants / data sources / materials
- Procedures or protocols
- Analytical framework (qualitative, quantitative, mixed methods)]

5 FINDINGS

[Present your results in a clear, logical, and concise manner. Use tables, figures, or visuals where appropriate. Ensure all figures and tables are properly labeled and referenced in text. Do not interpret results extensively here—that belongs in the discussion.]

6 DISCUSSION

[Interpret your findings in relation to prior studies, theory, and practice. Discuss:

- What do the results mean?
- How do they compare with existing research?
- What are the implications and open questions?
- What are the limitations of your study? (briefly)
- What future work does this suggest?]

7 IMPLICATIONS FOR CYBER DEFENSE

[As part of the discussion, or as a separate subsection, explain specifically how your work informs the field of cyber defense. What are the operational, strategic, policy, or technological implications? How can military, industry, or government stakeholders apply your insights?]

8 CONCLUSION

[Summarize the main contributions of your work, highlight the significance of the findings, and restate their relevance to cyber defense. Keep concise. Avoid introducing new results]

PROFESSIONAL COMMENTARY RECOMMENDATIONS

INTRODUCTION

The introduction should briefly place your commentary in context and explain why it matters. Since professional commentaries are practice-oriented, the introduction should balance relevance for practitioners and accessibility for a broad readership.

Suggested guiding questions:

- What is the challenge, opportunity or strategic issue you are addressing? Who is impacted, and in what mission or context?
- Why does it matter now? Emphasize timeliness by connecting to – and drawing on evidence from – recent conflicts, events, adversary actions, technological advances, doctrinal changes, or current defense priorities (e.g., resilience, deterrence, force generation).
- What is your perspective or experience? Briefly summarize the lens of your experience—military command, operational planning, acquisition, cyber operations, policymaking, etc.— and how this grounds your insights.
- What is the unique value of your commentary? Are you offering lessons from the field, operational reflections, or policy insights that can inform strategy, doctrine, or capability development? Clarify whether you are offering insights from practice, reflections from experience, or provocative arguments to spark discussion? Emphasize the relevance for key defense stakeholders: who might benefit from reading this piece (e.g., military forces, defense industry, policymakers)?

MAIN BODY

The body can be structured flexibly, but it should follow a logical flow. Use clear headings to help readers navigate the commentary. Possible elements include:

- **Context and background**: Provide additional historical, geopolitical, technical, or conceptual background if necessary. Clearly define key concepts that are used throughout the paper.
- **Author's Perspective**: Bring in your own practice-based insights, experiences, or lessons learned. This is a hallmark of this format. The experience, perspective, or professional role of the author(s) is central to the value of the piece. Readers and reviewers alike benefit from knowing the authority and practical background behind the arguments presented.
- **Analysis and reflection**: Engage with relevant literature, frameworks, or prior discussions to support and enrich your points. Avoid simply descriptive writing—show implications, contrasts, or lessons.

DISCUSSION / IMPLICATIONS FOR CYBER DEFENSE

- Draw out the practical insights: What are the operational, strategic, policy, or technological implications? What should military, industry, or government stakeholders take away from this commentary?
- Highlight challenges, risks, or opportunities that deserve further attention.
- Situate your reflections in the broader cyber defense landscape: what is new, provocative, or valuable?

CONCLUSION

Summarize your key message and its relevance to cyber defense in a strong closing statement. Optionally, end with recommendations or questions for future discussion.

ABOUT THE AUTHORS

Author 1 First Name Last Name insert your short bio here (150 words max.).

Author 2 First Name Last Name insert your short bio here (150 words max.).

Author 3 First Name Last Name insert your short bio here (150 words max.).

ACKNOWLEDGMENTS

Acknowledgments are hidden when the document class is set to *review*. They will be added to manuscripts accepted for publication. Acknowledgments are not compulsory. Where included, they should be brief. Grant or contribution numbers may be acknowledged.

REFERENCES

Distler, Verena, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. "A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research." *ACM Trans. Comput.-Hum. Interact.* (New York, NY, USA) 28, no. 6 (December). ISSN: 1073-0516. https://doi.org/10.1145/3469845. https://doi.org/10.1145/3469845.

GAO (U.S. Government Accountability Office). 2020a. *Climate Resilience: DOD Coordinates with Communities, but Needs to Assess the Performance of Related Grant Programs (GAO-21-46).* GAO (December 2020), pp. 13–15. https://www.gao.gov/assets/gao-21-46.pdf.

GAO (U.S. Government Accountability Office). 2020b. *DOD Utilities Privatization: Improved Data Collection and Lessons Learned Archive Could Help Reduce Time to Award Contracts (GAO-20-104).* GAO (April 2, 2020). https://www.gao.gov/products/gao-20-104.

Sánchez Chamorro, Lorena, Romain Toebosch, and Carine Lallemand. 2024. "Manipulative Design and Older Adults: Co-Creating Magic Machines to Understand Experiences of Online Manipulation." (Copenhagen, Denmark), DIS '24, 668–684. https://doi.org/10.1145/3643834.3661513. https://doi-org.proxy.bnl.lu/10.1145/3643834.3661513.

Sanger, David E. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.* Crown Publishers.

U.S. Department of Defense. 2018. *The Department of Defense Cyber Strategy.* https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf.

A APPENDIX A: EXAMPLES REFERENCE LIST ENTRIES

Book

Sanger, David E. 2018. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown Publishers.

Book Chapter

Sandvik, Kristin B. 2016. "Law in the Militarization of Cyberspace: Framing a Critical Research Agenda." In Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives, edited by I. K.Friis and J. Ringsmose, 175–197. Routledge

Journal article

Harknett, Richard J., and Max Smeets. 2020. “Cyber Campaigns and Strategic Outcomes.” Journal of Strategic Studies 45 (4): 534-567. https://doi.org/10.1080/01402390.2020.1732354

Conference paper

Craig, Anthony, and Brandon Valeriano. 2016. “Conceptualising Cyber Arms Races.” In 2016 8th International Conference on Cyber Conflict: Cyber Power, edited by N. Pissanidis, H. Rõigas, and M. Veenendaal, 141–158. Tallinn, Estonia: NATO CCD DOE Publication.

News or magazine article

Irwin, Sandra. 2021. “DoD Space Agency: Cyber Attacks, Not Missiles, Are the Most Worrisome Threat to Satellites.” Space News, April 14. https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites

Thesis or dissertation

Hauptman, Allyson. 2024. “The Human Side of Adaptive Autonomy: Design Considerations for Adaptive Autonomous Teammates.” PhD dissertation, Clemson University.

Web page

It is often sufficient to describe websites in the text (“As of November 15, 2023, Google’s privacy policy stated . . .”) or as a footnote. If a more formal citation is needed, it may be styled like: Google. 2023. “Privacy Policy.” Privacy and Terms. Effective November 15. https://policies.google.com/privacy.

Directive / Instruction

Department of Defense. 2019. “DoD Instruction 8500.01: Cybersecurity.” DoD Chief Information Officer, October 7. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

Doctrine / Field Manual / Military Regulation

Joint Chiefs of Staff. 2017. Countering air and missile threats. JP 3-01, Washington, DC, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Strategy Document

U.S. Department of Defense. 2018. The Department of Defense Cyber Strategy. https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf

Received Day Month Year; Revised Day Month Year; Accepted Day Month Year