US-China Foreign Language, April 2026, Vol. 24, No. 4, 169-174
doi:10.17265/1539-8080/2026.04.005

A Study on English-Chinese Translation Strategies for Cybersecurity Terminology

JIAO Yatong, GAO Jun
University of Shanghai for Science and Technology, Shanghai, China

Cybersecurity has emerged as a critical global concern. The accurate translation of technical terminology is essential for the effective dissemination and application of cybersecurity technologies. Based on the Chinese translation of *How to Solve Cybersecurity Once and For All*, this paper explores the linguistic features of cybersecurity terminology. Guided by technical translation principles featuring technical precision, industrial standardization and readability balance, this study analyses linguistic attributes of cybersecurity terminology and divides them into four categories: conceptual terms, coined terms, abbreviations, and polysemous pragmatic terms. Accordingly, four corresponding translation strategies are proposed: normative equivalence, conventional reconstruction, explicitation with retention, and contextual adaptation. The constructed "Feature-Classification-Strategy" framework provides systematic and standardized references for English-Chinese translation practice of cybersecurity terminology.

Keywords: cybersecurity terminology, translation strategies, semantic equivalence, industry standards

Introduction

In the digital age, cybersecurity terminology serves as the primary vehicle for technical communication and global collaboration. The accuracy of these translations directly influences the implementation of security protocols and the effectiveness of international defensive practices (Ma, 1997). *How to Solve Cybersecurity Once and For All*, published in *IEEE Security & Privacy* (Böhme, 2025), is an authoritative invited expert perspective article. It contains about 2,800 English words and covers issues, such as vulnerability mechanisms, security defense, formal verification, and security engineering. A total of 92 key terms are extracted and classified into four categories. While traditional technical translation principles emphasize "accuracy, normativity, and conciseness" (Ma, 1997), the dynamic and multidisciplinary nature of cybersecurity demands a more nuanced approach. This paper analyzes the "Feature-Classification-Strategy" chain of cybersecurity discourse and argues that a one-size-fits-all translation model is insufficient. Instead, a diversified strategic toolkit is required to navigate the spectrum between stable cryptographic theories and dynamic, context-dependent attack vectors.

Characteristics and Classification of Cybersecurity Terminology

Characteristics

Cybersecurity terminology is a multidisciplinary technical lexicon integrating computer science, cryptography and software engineering, with distinct linguistic and pragmatic features.

JIAO Yatong, postgraduate student, College of Foreign Languages, University of Shanghai for Science and Technology, Shanghai, China.
GAO Jun, Ph.D., professor, College of Foreign Languages, University of Shanghai for Science and Technology, Shanghai, China.

First, the terminology features high semantic precision and stability. Key terms, such as formal verification and hash function carry fixed technical definitions and clear referential boundaries, which require accurate and standardized translation.

Second, the terminology demonstrates active neologism and strong metaphoricity. Driven by emerging cyber threats and attack methods, a large number of novel metaphorical terms, such as jailbreak, Spectre, and zero-day keep emerging, reflecting the dynamic and confrontational nature of the cybersecurity field.

Third, the terminology makes extensive use of abbreviations for communicative efficiency. Acronyms, such as static application security testing (SAST), dynamic application security testing (DAST), and common vulnerabilities and exposures (CVE) are widely employed to compress information and facilitate professional communication.

Fourth, many technical terms exhibit obvious context dependency and polysemy. Terms like exploit, compromise, and vector change their specific meanings with technical scenarios and syntactic functions, belonging to typical context-sensitive pragmatic terms.

Classification

Based on the above linguistic features and terminological principles of non-literary translation emphasizing accuracy, standardization, and context appropriateness, this study establishes a four-tier functional taxonomy in accordance with semantic stability, word-formation mechanisms, context dependency, and standardization level. The classification corresponds to translation practice and provides clear guidance for strategy selection.

The first category comprises conceptual terms, which form the theoretical bedrock of the field, e.g., speculative execution, access control, and formal verification. These terms are logically rigorous, semantically stable, and consistent with industrial standards, serving as the fundamental concepts of cybersecurity.

The second category consists of coined terms, which are often metaphorical labels for emerging technologies and vulnerabilities, e.g., phishing, Meltdown, honeypot, and RowHammer. These terms are vivid, innovative, and lack unified standard translations in the early stage, requiring conventional reconstruction and semantic reproduction.

The third group involves abbreviations, which are highly compressed forms for professional efficiency, e.g., DDoS, MFA, API, and APT. They are widely used in technical discourse and need to be translated through explicitation and abbreviation retention to ensure accuracy and readability.

The final category includes polysemous pragmatic terms, such as bypass, compromise, mitigation, flaw, and isolation. Their meanings vary greatly across technical scenarios and syntactic environments, demanding context-driven adaptation and flexible selection of equivalents.

This taxonomy provides a systematic framework for selecting targeted translation strategies in the following sections.

Translation Strategies for Cybersecurity Terminology

Derived from the linguistic attributes and categorical differences of cybersecurity terminology summarized above, terms extracted from the article exhibit distinct semantic connotations, structural forms, and pragmatic functions. It is therefore inappropriate to adopt a unified translation approach in rendering all terminology. Based on the English-Chinese translation practice of *How to Solve Cybersecurity Once and For All*, this section elaborates on four targeted translation strategies applicable to the terminology in the source text, with specific illustration of practical application scenarios and operational considerations.

Normative Equivalence

Conceptual terms constitute the fundamental theoretical terminology of cybersecurity, featuring fixed disciplinary definitions, stable semantic connotations, and unified internal logical relations. Within the selected *IEEE* article, such terms serve as the basic carrier of professional theoretical narration, and their translation prioritizes the principle of normative equivalence. The core requirement of this strategy is to follow existing industrial specifications and acknowledged professional expressions, ensuring that the translated version completely matches the source term in conceptual denotation and disciplinary connotation without arbitrary addition or omission of meaning.

Semantic equivalence is the core principle of technical terminology translation, which demands full consistency in conceptual scope and logical implication between source and target terms. For conceptual terms with clear and fixed technical definitions, literal translation is the optimal method to guarantee lexical accuracy and conceptual integrity. As S. Guo and J. Guo (2015) emphasized, semantic equivalence requires a one-to-one correspondence between technical concepts and their internal logical connotations. For example, "memory-safe languages" is translated as "内存安全语言," which directly corresponds to the programming language that can avoid memory leakage vulnerabilities; "threat modelling" is rendered as "威胁建模," accurately expressing the process of analyzing and predicting potential system security threats.

For compound conceptual terms, the decomposition translation method is applicable: translate each core component separately, and then combine them in line with Chinese technical writing norms. For instance, "secure-by-construction" is translated as "构建即安全," which highlights the core meaning of embedding security attributes in the system construction stage; "proof-carrying code" is rendered as "带证明代码," which conforms to the fixed professional expression in the field of cryptography and fully retains the technical connotation.

In addition, terms, such as symbolic execution, abstract interpretation, and threat modeling all fall into this category of theoretically grounded terminology. Their translation should adhere to standardized equivalents while maintaining internal consistency across the terminological system. In general, the translation of concept-based terms should follow the principle of "norm-oriented and predominantly literal translation," thereby ensuring the accurate transmission of technical meaning through maximal preservation of the original logical structure.

Conventional Reconstruction

In contrast to conceptual terms, coined terms typically emerge from the cutting edge of technological development and are often characterized by vivid imagery and metaphorical expression. Owing to the absence of standardized translations at their initial stage, translators must strike a balance between adherence to established conventions and faithful semantic representation.

In *The Selected Article*, Spectre and Meltdown exemplified typical vulnerability names. Although derived from everyday vocabulary, these terms acquire specialized meanings within cybersecurity contexts. "Spectre, meaning ghost," metaphorically conveys the stealth and invisibility of the attack, and is therefore translated as "幽灵漏洞." "Meltdown," originally referring to "collapse or breakdown, highlights the failure of security mechanisms" and is rendered as "熔断漏洞." Such translations go beyond literal equivalence and instead involve semantic reconstruction grounded in technical understanding, while preserving metaphorical resonance.

Similarly, "RowHammer" denoted a hardware attack involving repeated access to memory rows that induces bit flips. Its conventional translation, "行锤漏洞," retains both imagery and mechanism, whereas a mechanically

literal version, such as “行锤击” would weaken its terminological stability. Likewise, “jailbreak” has been widely standardized as “越狱,” a rendering derived from metaphorical extension and firmly established within industry usage.

Accordingly, as Wen and Qiu (2010) suggested, such translations should aim for semantic reproduction while adhering to industry norms to ensure the terms are widely accepted. In the absence of standardized equivalents, a combined approach of transliteration and semantic translation may be employed. The guiding principle is to base translation on industry convention while aiming at semantic reconstruction, thereby ensuring both intelligibility and the preservation of metaphorical and technical features.

Explicitation with Abbreviation Retention

Abbreviations are extensively used in cybersecurity texts to enhance communicative efficiency, yet they may also pose challenges to comprehension. Translation must, therefore, balance professional precision with reader accessibility.

The cybersecurity domain has developed a substantial body of standardized terminology, supported by national standards, such as GB/T 25069-2022. Translators should prioritize these conventions to ensure consistency. For well-established abbreviations and core terms, conventional renderings should be directly adopted-for example, “API” as “应用程序编程接口” and “Pwn2Own” as “黑客攻防大赛.”

For emerging abbreviations, translation should follow analogous conventions to maintain consistency. For instance, “SAST” and “DAST” are appropriately translated as “静态应用程序安全测试 (SAST)” and “动态应用程序安全测试 (DAST).” This “full-form translation plus abbreviation retention” strategy ensures semantic completeness while preserving internationally recognized forms, thus facilitating subsequent comprehension.

Similarly, “CVE,” as a globally standardized naming system, is rendered as “通用漏洞披露编号 (CVE),” in accordance with established norms. Such terms should strictly follow standard usage rather than being arbitrarily altered.

It should also be noted that the treatment of abbreviations depends on text type and target readership. Academic writing typically requires full explanation upon first occurrence, whereas technical documentation may directly employ abbreviated forms. Thus, abbreviation translation is not merely a linguistic issue, but also a matter of communicative strategy. The principle of “explication upon first occurrence and retention thereafter” effectively reconciles informational completeness with communicative efficiency. As Ding (2000) noted, adhering to industry routines is essential for standardized terminology translation.

Context-Driven Adaptation

Polysemous pragmatic terms pose the greatest challenge in cybersecurity translation, as their meanings—and sometimes grammatical functions—vary across contexts. As such, translation cannot rely on fixed equivalence but must be dynamically adjusted in accordance with contextual factors.

Drawing on Hu’s (2008) Adaptation and Selection Theory, terminology translation should adapt to contextual requirements and flexibly adjust according to grammatical function and technical scenario. For polysemous terms, translation should be determined by syntactic role. For example, “flaw” is rendered as “安全漏洞” in “security flaw,” but as “缺陷” in “flaw in the defense;” “compromise” is translated as “破坏安全” when “functioning” as a verb and “安全受损” when used as a noun.

For polysemous pragmatic terms, translation should align with specific technical scenarios. For instance, “sandboxing” may be rendered as “沙箱技术” in “software security contexts,” but as “沙箱隔离” in “attack-

defense scenarios;" "isolation" may be translated as "硬件隔离" or "网络隔离," depending on context.

In complex sentence structures, an integrative translation strategy may be adopted. For example, "undefined behavior in the gap between source code and executable" is translated as "源代码到可执行文件转化过程中的未定义行为," which ensures semantic completeness while conforming to Chinese technical discourse conventions.

Take exploit as an illustrative case: It may denote either a "漏洞利用程序" or the act of exploiting vulnerabilities. A uniform translation would either obscure its technical specificity or lead to semantic inconsistency. Therefore, the translator must determine the appropriate rendering based on syntactic structure and contextual function.

Similarly, "mitigation" may be translated as "缓解措施" in "defensive contexts," or as "风险缓解机制" in "system design or risk management contexts." The term "attack" may refer either to "a general action" or to "a specific method or model," necessitating context-sensitive renderings, such as "攻击" or "攻击方法."

In essence, the translation of polysemous pragmatic terms constitutes a context-driven process of dynamic selection, requiring careful syntactic and semantic analysis to achieve functional equivalence. Only through a thorough understanding of context can the translator avoid the inaccuracies associated with mechanical equivalence.

Conclusion

Based on the Chinese translation of the selected academic article, this paper analyzes the linguistic features of cybersecurity terminology extracted from this article and categorizes the terms into four types: conceptual terms, coined terms, abbreviations, and polysemous pragmatic terms. Corresponding to the four term categories, this paper proposes four targeted translation strategies: normative equivalence, convention-based reconstruction, explicitation with abbreviation retention, and context-driven adaptation, establishing a localized analytical framework of "feature-classification-strategy" suitable for the terminology in this specific text.

The analysis reveals that the cybersecurity terminology in the chosen article presents unique lexical and contextual traits. In translation, it is essential to balance accuracy, standardization, readability, and professionalism. Terms of different categories ought to be handled with tailored strategies, so as to achieve satisfactory semantic and functional equivalence in the Chinese version.

This research also has limitations due to its single-corpus design.

Firstly, the discussion is only based on one academic journal article, and does not cover technical manuals, industry reports, or practical documents of cybersecurity.

Secondly, the study relies solely on qualitative textual analysis of selected typical terms, with no empirical or quantitative verification.

Thirdly, as cybersecurity technology develops rapidly, new terminology keeps emerging. This paper can only reflect the lexical features of the chosen text at the current stage, leaving the translation rules of emerging terms for further exploration.

References

Böhme, M. (2025). How to solve cybersecurity once and for all. *IEEE Security & Privacy, 23*(3), 79-82. https://doi.org/10.1109/MSEC.2025.3551590

Ding, S. (2000). On conceptual positioning and translation principles of scientific terminology. *Chinese Science & Technology Translators Journal, 13*(1), 14-16.

Fan, C. Y., & Zhong, H. C. (2003). An analysis of scientific and technical terminology translation. *Chinese Translators Journal, 24*(1), 59-61.

Guo, S. L., & Guo, J. (2015). Translation of scientific terminology from the perspective of functional equivalence theory. *China Terminology, 17*(3), 28-31.

Hu, G. S. (2008). Translation theories from the perspective of terminology: An overview of adaptation and selection theory. *Shanghai Journal of Translators, 23*(2), 1-5.

Leng, B. B. (2012). An analysis of typical problems in scientific and technical translation. *Chinese Science & Technology Translators Journal, 25*(3), 8-11.

Ma, Q. H. (1997). On the standards of scientific translation and principles of terminology translation. *Chinese Translators Journal, 18*(1), 28-29.

Wei, M. F. (2014). Lexical features and translation of English scientific and technical terminology. *Chinese Science & Technology Translators Journal, 27*(1), 5-7 & 23.

Wen, X. M., & Qiu, F. Y. (2010). Convention and innovation in the translation of scientific and technical terminology. *Chinese Science & Technology Translators Journal, 23*(3), 13-15 & 19.

Zhang, X. (2004). On the Chinese translation of translation studies terminology. *Chinese Translators Journal, 25*(6), 83-86.