Aysel Shabanova
Azerbaijan State Oil and Industry University

10.30546/2518-752X.1.507.024

TECHNICAL ENGLISH TERMINOLOGY IN CYBERSECURITY

Keywords: *Cybersecurity, Technical English, Terminology, Information Security, Translation*
Açar sözlər: *Kibertəhlükəsizlik, Texniki İngilis dili, Terminologiya, İnformasiya təhlükəsizliyi, Tərcümə*
Ключевые слова: *кибербезопасность, технический английский, терминология, информационная безопасность, перевод*

Introduction

In the digital era, cybersecurity has emerged as one of the most critical domains across both public and private sectors. As global communication becomes increasingly dependent on English, technical English serves as the backbone of information transfer in highly specialized fields such as cybersecurity. Technical English in this context refers not only to the standard English language, but also to domain-specific terminology, structured syntax, and functional clarity that support accurate communication of security processes, protocols, and risk analysis.

Cybersecurity professionals, engineers, analysts, and educators rely heavily on a precise and shared understanding of technical terms. These terms describe processes such as encryption, penetration testing, authentication, data breaches, and malware mitigation. Furthermore, the importance of this terminology goes beyond communication – it underpins the understanding of tools, documentation, and international standards that guide digital safety.

Despite its importance, learning and using technical cybersecurity English presents multiple challenges, particularly for non-native English speakers. Acronyms, compound terms, context-dependent vocabulary, and rapid innovation in the field create a complex linguistic environment. This article examines the core technical terms used in cybersecurity, analyzes the challenges of mastering them, and offers pedagogical strategies for teaching technical English in this domain. It draws upon both English-language literature and Azerbaijani-language academic sources to provide a comparative perspective.

The Role of Technical English in Cybersecurity

Technical English functions as a crucial tool for operational clarity and precision in cybersecurity environments. Its primary role is to enable consistent understanding of digital threats, defenses, tools, and protocols. Without standardized and widely accepted terminology, international cooperation in cybersecurity would be severely hindered.

Cybersecurity involves an array of specialized disciplines – network security, data protection, ethical hacking, cyber forensics, and more. Each subfield contains highly specific terminology that must be interpreted precisely. Terms like firewall, encryption, DDoS attack, and zero-day vulnerability each carry technical implications that require users to understand both the linguistic form and the practical function of the term. For instance, misunderstanding the term phishing might lead a user to underestimate the severity of a social engineering attack [4].

Furthermore, technical English contributes to the effectiveness of documentation. Manuals for intrusion detection systems (IDS), protocols for vulnerability testing, and cybersecurity policies are often published in English, even in non-English-speaking countries. As a result, professionals working in global companies or cross-border cyber teams must be proficient in this technical variant of English.

Technical English also enhances machine-to-human communication. Command-line interfaces, error messages, and log files all rely on structured English that is minimalistic but highly technical. Training cybersecurity professionals to correctly interpret such information is vital for prompt and correct decision-making in response to incidents.

Common Terminology and Lexical Characteristics

Cybersecurity terminology is characterized by its precision, functional specificity, and rapid evolution. The field borrows terms from computer science, military jargon, and legal discourse, resulting in a complex technical vocabulary that requires systematic learning and contextual interpretation. Cybersecurity English is marked by certain linguistic traits:

- Frequent use of compound words (e.g., password manager, threat landscape)
- Proliferation of acronyms (e.g., VPN, SSL, SOC)
- Creation of neologisms and blends (e.g., smishing – a blend of SMS and phishing)

General English words often take on new meanings in technical contexts. For instance, the word cookie (in cybersecurity, a data file stored on a user's browser) has a different meaning than in everyday language.

Challenges for Non-Native Speakers

Mastering technical English terminology in cybersecurity poses significant challenges for non-native English speakers. These challenges are not only linguistic but also cognitive and contextual, as the domain requires fast adaptation to evolving technologies and vocabulary [1].

– Vocabulary Density and Abstraction

Technical cybersecurity language is dense and highly abstract. Words such as sandboxing, obfuscation, or hashing (refers to converting data into a fixed-size string using a mathematical function) require not only vocabulary knowledge but also conceptual understanding. For learners whose first language is Azerbaijani or another non-Germanic language, such concepts may not have direct equivalents, making translation difficult and sometimes misleading.

– Acronyms and Jargon

The excessive use of acronyms – such as SIEM (Security Information and Event Management), IDS (Intrusion Detection System), and PKI (Public Key Infrastructure) – can overwhelm learners unfamiliar with the context. Many

acronyms have overlapping meanings depending on the system or standard being used, creating confusion.

Additionally, cybersecurity professionals use jargon that may differ slightly even among English-speaking countries, let alone in translation. For example, the term bug bounty (a reward offered to individuals who identify security vulnerabilities) might be unfamiliar or misunderstood without proper contextualization.

Teaching and Learning Technical Cybersecurity English

The effective teaching of technical English in cybersecurity requires a blend of domain-specific knowledge, language instruction methods, and the use of authentic materials. Since the field constantly evolves, English for Specific Purposes (ESP) instructors must adapt their strategies accordingly.

Integration of ESP Methodology

English for Specific Purposes (ESP) focuses on the linguistic needs of learners within particular disciplines. In the context of cybersecurity, ESP emphasizes teaching learners how to comprehend and produce texts such as technical reports, manuals, threat analyses, and vulnerability assessments.

One effective approach is the task-based learning (TBL) model, where students perform real-world tasks such as:

- Writing an incident report on a simulated attack
- Analyzing and paraphrasing terms in a vulnerability disclosure
- Presenting security recommendations in English to a team

These tasks help students develop both linguistic and analytical skills essential in professional cybersecurity environments.

Use of Authentic and Multimodal Materials

To familiarize learners with real cybersecurity language, educators are encouraged to use:

- Security blog posts and threat intelligence feeds
- Video tutorials from platforms like Cybrary or YouTube
- Real or adapted security advisories from companies like Cisco or Kaspersky
- User interfaces of firewalls, antivirus programs, or encryption software

Such resources help students hear and see the actual terminology in action, improving both comprehension and retention.

Bilingual Glossaries and Comparative Lexical Practice

For Azerbaijani learners, developing bilingual glossaries can bridge the gap between native language understanding and English terminology [3]. For instance:

- Threat actor (təhlükə yaradan tərəf)
- Exploit (zəiflikdən istifadə edən proqram)
- Patch (təhlükəsizlik yeniləməsi)

These comparative glossaries can be student-generated as a classroom activity, encouraging deep processing of terms.

Collaboration Between Language and IT Specialists

ESP instructors benefit greatly from collaboration with IT professionals who can:

- Provide up-to-date terminology
- Help simulate real-world communication contexts
- Co-design curriculum that reflects practical industry needs

Joint efforts also support the standardization of English cybersecurity terms in Azerbaijani academic contexts.

Assessment Strategies

Assessment should not only focus on grammar or vocabulary recall but on:

• Clarity of written explanations of threats

• Correct use of terminology in oral presentations

• Ability to interpret and respond to professional security emails or system messages

Rubrics can be developed based on Can-Do Statements tailored to technical communication in cybersecurity.

Conclusion

As the digital world becomes increasingly interconnected and cyber threats grow more sophisticated, the role of English as the dominant language of cybersecurity continues to expand. Mastery of technical English terminology is not merely a linguistic goal but a functional necessity for professionals operating in this high-risk domain.

For Azerbaijani learners and educators, this requires a structured approach to English for Specific Purposes (ESP), the integration of authentic materials, and the development of bilingual resources. Overcoming challenges such as vocabulary overload, structural complexity, and lack of native-language materials will be essential in developing competent specialists who can engage confidently in global cybersecurity discourse [5].

Furthermore, collaboration between linguists, educators, and IT specialists is key to keeping teaching materials up to date and industry-relevant. With a balanced approach that includes terminology instruction, task-based learning, and real-world application, technical English in cybersecurity can be taught effectively and meaningfully – strengthening both linguistic and professional competence.

Purpose and Objectives of the Article

The main purpose of this article is to examine the technical English terminology used in the field of cybersecurity, analyze its origins and functional features, and explore its equivalents in the Azerbaijani language. The article also aims to highlight the role of technical terminology in ensuring effective professional communication within cybersecurity contexts.

Objectives: to identify and classify the key technical terms commonly used in cybersecurity; to analyze the linguistic structure and semantic features of selected terms; To trace the etymology and sources of these terms (e.g., abbreviations, neologisms, borrowings); to compare English cybersecurity terms with their Azerbaijani counterparts; to evaluate the challenges of translating or adapting cybersecurity terminology into Azerbaijani.

Scientific Novelty of the Article

The scientific novelty of the article lies in its comparative approach to English and Azerbaijani technical terminology in the field of cybersecurity. While much research has been conducted on general ICT vocabulary, this study focuses specifically on cybersecurity, a rapidly evolving and increasingly vital subfield. The article introduces a linguistic framework for analyzing the structure and function of cybersecurity terms and offers original insights into the challenges of

bilingual term equivalence and translation. Additionally, it contributes to the development of localized terminology resources that can aid both academic research and practical application in Azerbaijan**.**

References:

1. Al-Rawi, A. (2020). Language and cybersecurity: Barriers for non-native speakers. Journal of Cyber Communication, 6(2), 112-123.
2. Choudhury, M. (2021). Terminology management in cybersecurity: A linguistic perspective. IT Terminology Review, 9(1), 45-53.
3. Həsənli, F., & Məmmədov, R. (2021). Kibertəhlükəsizlik terminləri və tərcümə problemləri. Bakı: Elm və Təhsil.
4. Kaspersky. (2022). What is Cybersecurity? Retrieved from https://www.kaspersky.com /resource-center/definitions/what-is-cyber-security
5. Quliyev, E. (2022). Texniki terminlərin Azərbaycan dilində istifadəsi: Kibertəhlükəsizlik nümunəsində. Bakı: Dil və Terminologiya Jurnalı.

Aysel Şabanova

Xülasə

KİBER TƏHLÜKƏSİZLİKDƏ TEXNİKİ İNGİLİS TERMİNOLOGİYASI

Bu məqalədə kibertəhlükəsizlik sahəsində texniki İngilis dili terminologiyasının inkişafı və istifadəsi araşdırılır. İngilis dilinin texnologiyanın qlobal dili kimi rolu və terminlərin Azərbaycan dilinə tərcümə və uyğunlaşdırılması məsələləri müzakirə olunur. Məqalədə həmçinin İngilis və Azərbaycan dillərindəki bəzi terminlərin müqayisəsi aparılır və təhsil və sənayedə terminologiyanın standartlaşdırılmasının əhəmiyyəti vurğulanır.

Айсел Шабанова

Резюме

АНГЛОЯЗЫЧНАЯ ТЕХНИЧЕСКАЯ ТЕРМИНОЛОГИЯ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

В статье рассматривается развитие и использование англоязычной технической терминологии в области кибербезопасности. Также анализируется роль английского языка как глобального языка технологий, и способы перевода и адаптации терминов на азербайджанский язык. Дополнительно, проводится сравнение терминов на английском и азербайджанском языках и подчеркивается важность стандартизации терминологии в сфере образования и промышленности.

Rəyçi: prof. İ.Z.Qasımov