JEZIKOSLOVLJE
27.1 (2026): 289-313

UDK 811.111'42=111
Izvorni znanstveni članak
Prihvaćen za tisak 7. 1. 2026.
https://doi.org/10.29162/jez.2026.11

Adriana Petra Blažević
Filozofski fakultet Sveučilišta u Splitu

Cybersecurity Discourse: A CDA of Western Perspectives on Cyber Threats

This paper argues that the discursive practices surrounding cybersecurity are infused with ideology and often deviate from principles of objectivity and accuracy. The research offers a critical analysis of three speeches delivered by government officials from the United States, the United Kingdom, and Australia. Using the framework of Critical Discourse Analysis (CDA), the study draws on Van Dijk's concepts of local and global meanings, Wodak's and Fairclough's approaches to intertextuality, and Van Dijk's ideological square. The findings reveal that by framing the cybersecurity narrative within a criminal context, Western powers position themselves as arbiters of justice. Cybersecurity threats are depicted as ongoing and immediate, with progressive forms and emotionally charged language amplifying their urgency. Intertextual analysis shows that discourse on cyberspace leverages past terrorist incidents and current geopolitical conflicts to induce fear and stoke animosity toward particular social groups. The analysis uncovers a problematic use of military terminology, despite the absence of actual warfare in cyberspace. Nation-states are personified as culprits, with cyberattacks construed as manifestations of their desire to undermine democracy and impose global dominance. This overarching narrative invites critical scrutiny, as it reveals a deepening polarisation between the West and East that aggravates long-standing geopolitical divides. As this language shapes our understanding of reality, such divisions risk transforming imagined threats into self-fulfilling prophecies. Ensuring terminological precision and conceptual clarity is therefore essential to recognising and resisting the manipulative potential of cybersecurity discourse.

Keywords: cybersecurity, critical discourse analysis, ideology, global meaning, local meaning, intertextuality

1. Introduction

Cyberspace is composed of computer networks that rely on the Internet but extend far beyond it (Clarke & Knake, 2014). The term has spatial implications, yet this *virtual* world defies geographic boundaries (Mahmoud, 2013). Despite challenges with attribution and intangibility, activities within cyberspace are often regulated to achieve specific objectives in the material world. Intentional breaches of cyber policies, such as network penetration, espionage or sabotage, are subsumed under the term *cyberattack*. Even when cyberattacks appear to be minor nuisances, an aura of secrecy surrounds the phenomenon and often fuels narratives of world domination unfolding in cyberspace.

The concept of *cybercrime* gained traction in the 1970s and has since evolved to encompass the contemporary surge in large-scale cyberattacks. Rid (2012) interprets the growing abuse of cyberspace as a predictable outcome of rapid technological advancement. Yet the emergence of new forms of crime cannot be fully understood in technical terms alone, as our grasp of cyber phenomena is always mediated through discourse. Language is inseparable from human cognition, and is shaped by internalised, ideologically nuanced mental frameworks that reveal collective attitudes, beliefs, and norms (Van Dijk, 2005). When applied to the cyber domain, this relationship between language and thought becomes particularly complex. Cyber realities are fluid, opaque, and often deliberately obscured, making them difficult to conceptualise using existing linguistic categories. Much of this vocabulary has been borrowed from legal, business, and military contexts in an attempt to ground unfamiliar concepts in familiar frames (Ramirez & Choucri, 2016). As this occurs against an ideological backdrop, Fairclough (2013b) cautions against the dangers of recontextualising discourse by drawing from other discursive domains. This is highly relevant to the cyber sphere, where such borrowing has produced a lexicon riddled with ambiguity, especially surrounding highly contested terms such as *cyber war* and *cyber warfare*.

Hunker (2010) broadly defines cyber warfare as a spate of disruptive cyber-attacks between nations. Classified as such, these attacks are subject to the laws of traditional warfare. This has allowed a proliferation of security-focused rhetoric, not only in interstate politics but in everyday life, where routine reminders about passwords and data protection reinforce a constant sense of vulnerability. As (Mauro, 2024) argues, the cybercrime ecosystem is inherently enticing and deceptive, which ensures that the language surrounding it remains speculative. In his words "the proliferation of deceptive online communications, be it cybercriminals phishing for credentials or nation-state disinformation campaigns, serves to maintain the status quo by leveraging appeals to power and authority for manipulation and influence" (p. 11).

Understanding how such mechanisms operate requires a method capable of uncovering the ideological work performed through language. To this end, this study adopts the methodological framework of Critical Discourse Analysis (CDA) and avails itself of the toolkit provided by Fairclough (1992; 2005; 2001) and Van Dijk (1976; 1980; 2001; 2011a) to appraise modern Western discourse on cybersecurity. It respects CDA's interdisciplinary foundations in rhetoric, philosophy, linguistics, and sociopsychology and applies Wodak's (2001; 2014) sociohistorical approach to assess how seemingly coincidental references derive meaning from their broader context. Within this framework, the analysis focuses on how language constructs intra-Western solidarity, defines the relationship between cyber *attackers* and *victims*, and represents both allied actors and perceived adversaries.

2. Theoretical Background

Discourse analysis focuses on discourse as a mechanism shaping and sustaining social reality (Fairclough & Wodak, 1997). Critical Discourse Analysis (CDA) places linguistic studies within social contexts but examines this interplay through a critical lens. Social critique, in this framework, extends beyond mere description and attempts to evaluate social dynamics against constructed standards of inequality (Fairclough, 2013).

Van Dijk (1980) proposes a layered approach to discourse analysis and focuses on macro, or global structures based on "how language users and social participants perceive, interpret, know, memorize, evaluate, plan, produce, etc., their discourses and interactions" (Van Dijk, 1980, p.2). He parallels the global/local distinction with a holistic/constitutive approach to discourse. Coherence, however, is maintained throughout, even as localised details fade to declutter semantics. These details, though obscured, remain traceable upon closer examination and allow for a deeper understanding of language.

Van Dijk (2011a) further relates cognitive or mental models to semantic structures at all levels, while describing words and sentences as semantically loaded constructs which imply rather than explicitly state the bulk of their meaning. Semantic comprehension thus runs much deeper than surface-level expression, with mental models shaped not only by the immediate communicative context but also, often implicitly, by sociocultural identity and the ideologies it carries. Macrostructures reflect both the speaker's understanding of discourse and the strategies employed to distil the most relevant content. Essentially, they use semantics to coherently bridge the discursive local (lexis and syntax) with the global and pave the way for different social, cognitive, and linguistic dimensions (Van Dijk, 1976).

Lexis and syntax are the building blocks of meaningful discourse, which, when properly aligned, ensure cohesion and coherence. As speakers engage in cognitive

processes such as interpretation, perception, and memorisation at both local and global levels (Van Dijk, 1980), the extraction of macrostructures based on micro-level semantics can cause the boundaries between global and local semantics to blur and even overlap, depending on the semantic role performed within the discourse. Nevertheless, analysing lexis and syntax is essential for drawing inferences at global levels, since macrostructures are derived from microstructures and, when elevated to a global scale, facilitate the understanding of discourse. While sentences occupy higher hierarchical levels, they are interpreted within localised semantic contexts. Inferencing occurs at both levels, but macroanalysis enables the synthesis of local propositions into global propositions. This process defines global themes through techniques such as deletion, selection, generalisation, and proposition construction, all of which function as means of filtering semantics (Van Dijk, 1980).

Discourse can be reduced only after thorough analysis, at which point its "implicit propositions" reveal the realm of the "unsaid" where ideologies reside (Fairclough, 2010, p. 26). Grasping ideology is inherently a social endeavour, as it comprises a collective set of beliefs, ideas, and values (Van Dijk, 2011). These shared beliefs possess a buoyant quality and often manifest in various forms across discursive practices. Van Dijk (1998) conceptualises the discursive infiltration of ideology through an *us* versus *them* polarisation, rooted in shared beliefs and strong assumptions of their legitimacy. Feelings of animosity are sustained by the four corners of the ideological square: positive self-representation, negative representation of the other, alongside the obscured negative representation of the self and the positive representation of the other.

To understand the dynamics that lead to the adoption of opposing beliefs and goals, it is crucial to consider the social and historical context surrounding the discourse. Wodak (2001) argues that an unbiased understanding of discourse can only be achieved after compiling and thoroughly analysing the historiographical facts that underpin it. This approach allows for a diachronic perspective, reveals the trajectory of discourse and explains how and why ideologies evolve or become stagnant. Contextualisation further supports intertextual analysis, which reveals layers of subtext and clarifies topical intersections. Intertextuality suggests that texts do not exist in isolation but rather reference one another while reflecting broader social contexts (Wodak, 2001; Fairclough, 1992). Wodak (2001) advocates a four-stage approach to critical discourse analysis: immediate analysis, intertextual analysis, contextual middle-range analysis, and finally, the capacity to situate these findings within the broader sociohistorical context. This method effectively restores the discourse to its rightful place with a deeper understanding of how it assumed its current form.

JEZIKOSLOVLJE
27.1 (2026): 289-313

3. The Geopolitical Context Surrounding Cybersecurity

Our understanding of cybersecurity has transformed over time. The digital landscape is no longer seen as a realm of unrestricted freedom, but as a domain governed by national and international policies (Kanik, 2011). Simons et al. (2024) highlight this shift by noting that cyberspace functions as both a resource and a vulnerability, which makes its discursive articulation a precarious undertaking. The portrayal of the cyber attacker has also shifted; cyber threats are no longer associated with isolated young enthusiasts working from their bedrooms but are now recognised as coordinated government operations. The discourse surrounding cybercrime has thus garnered substantial political significance, and cybersecurity is emerging as one of the foremost challenges for modern nations. Cyber safety talks at NATO's 2002 Summit in Prague paved the way for the integration of these issues into the first Cyber Defense Program (Fidler et al., 2013). Similar Western efforts have since manifested in a consistent rise in personnel, resources, and initiatives devoted to maintaining safety in cyberspace.

The US, UK, and Australia solidified these concepts in 2021 by forming AUKUS, a trilateral partnership focused on mutual collaboration in sharing nuclear submarines. The second pillar of this alliance tackles cyber security and addresses electronic warfare, the development of cyber and radar capabilities, and the exchange of advanced technology (*AUKUS: A Commitment to the Future*, 2023). In addition to the three AUKUS countries, the Five Eyes alliance includes New Zealand and Canada. As its name implies, the alliance seeks to unify intelligence agencies for defensive espionage and the dissemination of classified information. The People's Republic of China has repeatedly accused the network of harbouring a cold-war mentality to hinder its rise as a growing superpower (*Five Eyes Accustomed to Fabricating, Spreading Lies about China: Chinese FM - Global Times*, 2023).

Political discourse on cybersecurity has frequently affirmed and deepened ideological divides, with most large-scale cyberattacks attributed to China and Russia (Nagy, 2012; Bay, 2018). Their cooperation with the seemingly less powerful nations of Iran and North Korea has sparked serious discussions about the emergence of a *reinvigorated Axis of Evil* in cyberspace (Rugge, 2018). The blacklisting of Chinese tech companies Huawei and ZTE further escalated tensions and ignited claims of Chinese involvement in 5G infrastructure posing a national security threat (Zhou, 2023). Nevertheless, the three AUKUS member states see China as a crucial trade partner. Trade between the US and China has steadily intensified over the past fifty years, albeit disproportionately.[1] The mutually beneficial economic relationship between China and

[1] In 2022, the US exported $195.5 billion worth of goods to China, a pittance compared to the $562.9 billion in imports (Office of the United States Trade Representative, 2023).

Australia is particularly evident in the trade of iron ore, whereby Australia stands as the largest exporter and China as the largest importer (Granwal, 2024).

Russia became a designated cyber villain in 2007 after it reportedly launched a series of attacks disrupting Estonia's digital infrastructure. The relationship between Russia and the West, particularly the US, has often echoed Cold War rhetoric and has thus led to frequent standstills (Van Epps, 2013). Russia's 2022 invasion of Ukraine erased any prospects for improving Russo-Western relations and triggered a series of polarising measures.[2] Iran's cyber initiatives are closely tied to its nuclear program, as many Western efforts focus on undermining its uranium enrichment efforts (Anderson & Sadjadpour, 2018). In response, Iran has redoubled its efforts to enhance its defensive and offensive cyber acumen. North Korea has emerged as the fourth and reportedly least threatening cyber power. It primarily targets the cyberspace of South Korea and the United States, though its activities have generally been rudimentary, including email hacking, malware distribution, and mobile phone tapping. While North Korea remains a suspect on the West's blacklist, the secretive nature of its regime makes it difficult to assess its cyber capabilities (Boo, 2017).

The global dynamics outlined above offer a clearer understanding of international relations and provide a foundation for analysing discourse on cybersecurity. Fairclough (1992) and Wodak (2001) use the term intertextuality to describe this complex socio-historical-discursive interplay and emphasise its critical role in embedding new semantic structures within familiar contexts. Being attuned to both past and present social contexts is essential for understanding the ideological backdrop of any discourse, as it reveals much about the speaker and how effectively they weave historical references into their message.

4. Methodology

This research analysed three speeches[3] on cybersecurity delivered by government officials from the United States,[4] the United Kingdom,[5] and Australia.[6] All

[2] The economic sanctions have been particularly burdensome for the EU as 25% of its oil and 40% of its gas were imported from Russia (Hausmann et al., 2024). In contrast, the US was largely independent of Russian energy; in 2021, only 3% of its oil imports originated from Russia, with the majority sourced from Canada.

[3] All analysed transcripts are in the public domain and are not subject to copyright protection.

[4] Newman, D. (2024). *Principal Deputy Assistant Attorney General David Newman Delivers Remarks at 2024 U.S. Cyber Command Legal Conference*. (2024, April 17). Justice.gov. https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-david-newman-delivers-remarks-2024-us-cyber

[5] Keast-Butler, A. (2024). *CYBERUK 2024: Anne Keast-Butler keynote speech. (2024). Ncsc.gov.uk. https://www.ncsc.gov.uk/speech/cyberuk-2024-gchq-director-keynote-speech*

[6] Paterson, J. (2024). *Transcript | Speech to the AISA Canberra Australian Cyber Conference | 27 March 2024.* (2024). Senatorpaterson.com.au. https://www.senatorpaterson.com.au/news/transcript-speech-to-the-aisa-canberra-australian-cyber-conference-27-march-2024

three speakers hold significant roles in national cybersecurity: David Newman serves as the Principal Deputy Assistant Attorney General for the National Security Division at the US Department of Justice; Anne Keast-Butler is the Director of GCHQ, the UK's Intelligence, Cyber, and Security Agency; and Senator James Paterson is a Liberal Senator for Victoria, Australia and currently the Shadow Minister for Home Affairs, Cyber Security, and Cabinet Secretary. David Newman delivered remarks at the 2024 US Cyber Command Legal Conference in Maryland. His speech (referred to as Speech 1, or S1 hereafter), totalling 2,228 words, was broadcast live via the Defense Visual Information Distribution Service (DVIDS) platform. Anne Keast-Butler spoke at the 2024 CYBERUK Conference in Birmingham, organised by the UK government's National Cyber Security Centre (NCSC). Her 1,747-word address (referred to as Speech 2, or S2 hereafter) was streamed online. Senator Paterson delivered a 2,910-word speech (referred to as Speech 3, or S3 hereafter) at the 2024 Australian Cyber Conference in Canberra, which was also broadcast online.

All three conferences shared a common mission: advancing cybersecurity with an emphasis on international partnerships and public-private collaboration. The selected corpus is directly aligned with the core subject of this paper and is thus highly appropriate for this research. Its relevance is supported by the credibility (*ethos*) of the speakers and the context in which the speeches were delivered. Principles of Critical Discourse Analysis (CDA) were applied to analyse the discourse, with a distinct emphasis on semantic macrostructures, intertextuality and linguistic representations of actors in cyberspace. The following research questions guided the study:

1) How do semantic macrostructures shape Western discourse on cybersecurity, and in what ways do they connect to local meanings and lexical choices?
2) How do the speakers' intertextual practices construct intra-Western solidarity and what do these constructions reveal about the broader relationship between the West and the East?
3) How are the perpetrators of cyber-attacks addressed and linguistically represented in contrast to their victims?

In order to answer these questions, the following linguistic devices were considered:

- lexical choices
- figures of speech
- verb tenses and types
- active and passive voice
- modality
- pronoun selection

Examining these features enabled an understanding of how linguistic resources construct power relations within cybersecurity discourse. The study first outlines four semantic macrostructures identified in the data. The linguistic devices through which these macrostructures are realised are then analysed in terms of their persuasive force and ideological implications. The following section focuses on attribution in cyberspace, that is, how supposed cyber attackers are linguistically addressed and represented. Finally, conclusions are drawn about how such discourse delineates existing geopolitical divides.

Since this research is limited to Western discourse, it invites future work to look at comparable patterns emerging in other geopolitical contexts, including those of Russia or China. This is particularly relevant given that similar protectionist strategies have been observed there, ranging from the construction of threats to public safety and social order (Pigman, 2019), to appeals for safeguarding state sovereignty amid a perceived state of decline (Fung, 2022). Juxtaposing these perspectives would reveal the global reverberations of national cybersecurity discourse.

5. Semantic Macrostructures

After reducing the analysed discourse and elevating it to the level of semantic macrostructures, four key global propositions emerged. The list was compiled by adhering to Van Dijk's (1980) guidelines for discourse simplification, which involve the generalisation, deletion, and synthesis of key ideas. In accordance with his view that macrostructures are inferred from micro-level structures, the extraction of macro semantics was carried out through the analysis of specific language devices including local lexis, figures of speech, verb tense, voice, modality and pronoun use. The table below outlines the four semantic macrostructures drawn from the discourse, which are elaborated upon and substantiated by selected local structures in the following text.

Table 1 Higher-level macro propositions from the three speeches

1)	The cyber threat demands serious attention, having evolved significantly and continuing to advance in both complexity and scope (examples 1-11).
2)	Events in cyberspace ought to be interpreted through the lens of historical and ongoing conflicts between the West and the East (examples 12-14).
3)	The West maintains a moral high ground by addressing issues through legally authorised methods rather than resorting to crime (examples 15-18).
4)	Maintaining internal cohesion between government and the private sector, along with fostering genuine international partnerships, will be essential to securing the West's strategic edge (examples 19-22).

The first semantic macrostructure suggests that cyberspace is universally characterised as an interconnected landscape with unmatched potential for expansion. This is reinforced by the persistent dynamism of progressive forms (examples 1, 2 and 5), participial (examples 1, 2 and 6) and comparative (examples 3 and 4) adjectives, and intensifiers (examples 2, 5 and 6). David Newman's tricolon, reinforced by the alliteration of sibilant sounds (example 1), adds further weight to his argument:

(1) *Hostile adversaries are conducting cyber operations with alarming scale, speed, and sophistication.* (S1)

(2) *We are increasingly concerned about growing links between the Russian intelligence services and proxy groups to conduct cyber-attacks – as well as suspected physical surveillance and sabotage operations. Before, Russia simply created the right environments for these groups to operate but now they are nurturing and inspiring these non-state cyber actors.* (S2)

(3) *AI enables relatively unskilled threat actors to carry out more effective access and information-gathering operations.* (S3)

(4) *It's clear that technology and security are more tightly coupled than ever before.* (S2)

A heightened sense of urgency is clearly at play, and it reinforces the message about cybercrime as an immediate threat. This sets the stage for Anne Keast-Butler's appeal to authority in which she invokes the Prime Minister, a figure in whom significant power is concentrated:

(5) *But recent events remind us that our country and democratic institutions remain of interest to the Chinese authorities. We want to engage with China where it's mutually beneficial. Like tackling climate change, engaging in safe trade, and AI safety. It matters that China joined in signing the declaration on AI last November at Bletchley Park, the wartime home of GCHQ. But as the Prime Minister said recently… the leadership of the People's Republic of China, the PRC, is increasingly working with others to try and reshape the world.* (S2)

In this statement, the subject is represented through the collective noun *leadership*, which vaguely indicates a human component. However, the subsequent use of the abbreviation *PRC* institutionalises the agent and adds a layer of formality and detachment. The present continuous tense frames China's progressive efforts, and the intensifying adverb *increasingly* suggests potential escalation. China's actions are framed as deliberately disruptive, which provokes unease among those who wish to maintain the status quo. The statement is made more alarming by acknowledging that China is not acting alone; its partners are vaguely referred to as *others*,

implying a plurality of allies and highlighting China's leading role in this strategic collaboration. The discourse is crafted to warn the audience that unprecedented challenges lie ahead, and the figurative language (examples 6 and 7) intensifies the tone of an escalating threat.

(6) *We are at a crucial juncture for how we conceptualise national security risks in what is a rapidly evolving digital threat environment.* (S3)

(7) *And we need more prosecutorial horsepower to achieve the ambitious disruption goals in the National Cybersecurity Strategy.* (S1)

The metaphor of a *critical juncture* serves to assert both the immediacy of the moment and the imminent danger of making the wrong decision – that is, of *taking the wrong turn*. It establishes a clear binary between a right and a wrong path and implies that a failure to treat the issue with sufficient seriousness in the present will have detrimental consequences in the future. A second, equally powerful image emerges through the metaphor of *prosecutorial horsepower*. Although rooted in animal imagery, *horsepower* has long since migrated into technological and military domains, where it denotes operational capacity. In this context, the phrase combines legal and physical dimensions: *prosecutorial* implies institutional and judicial authority, while *horsepower* suggests strength and momentum, despite physicality having little direct relevance in cyberspace. While the expression acknowledges resource limitations, it simultaneously constructs a reassuring portrayal of the NSD as staffed by competent professionals equipped to confront these escalating cyber threats.

The supposed velocity of the *threats* is thus mobilised in a way to hinder the audience's ability to critically engage with the matter. Since the future is inherently uncertain, legitimation through fear (Wodak, 2001) is used to secure public compliance in the name of pre-emptive safety. Simons et al. (2024) describe this as the deliberate disorientation of audiences that provokes a demand for an urgent response. Duyvesteyn (2014) similarly notes that cyber narratives often swing between two extremes: doomsday and dismissal. In his delivery, Senator Paterson gravitates towards the doomsday end of the spectrum and invokes a near-apocalyptic scenario:

(8) *Failure will see us drift passively into an uncertain future, and I fear we will not truly understand the costs of this complacency until it is too late.* (S3)

He establishes a causal link between the nation's failure to engage proactively with cybersecurity and the severe consequences of such inertia. Epistemic modality further reinforces an aura of urgency and inevitability. Particularly notable is his choice of pronouns: the inclusive *us* and *we* convey collective accountability and a shared fate, while the personal pronoun *I* introduces an emotive, individual touch. The metaphorical use of the phrasal verb *drift into*, implying a loss of control over

one's trajectory, coupled with the alliterative phrase *cost of complacency* enhances both the memorability and emotional impact of the statement. However, the adverbial phrase *too late* creates a fabricated sense of dramatic finality despite the improbability of the situation truly descending into an irreversible crisis.

Privacy issues at a micro level, which have the potential to impact individuals across various demographics, were also addressed to underscore the critical significance of cyber threats in today's digital landscape.

(9) *Bulk data about an American's finances, for example, can be mined for leverage in coercion, blackmail, and espionage.* (S1)

As indicated by the use of epistemic modality, the tone of this statement is significantly less alarming than that of Senator Paterson's, with the modal verb *can* conveying a sense of reduced certainty. The passive construction of the sentence further obscures the agent and shifts focus away from those responsible for the data mining. The nominalisation and overuse of abstract terms further heighten the formality of the tone and tacitly add a layer of mistrust. The indefinite article *an* broadens the scope of potential cyber targets, while the phrase *for example* implies that the risks extend beyond those explicitly mentioned. The possessive form *American's* introduces a patriotic element and appeals to national sentiment. The sentence concludes with a memorable tricolon, under which all harmful activities are subsumed, leaving the audience with a lingering sense of unease.

Metaphors drawn from the realm of armed conflict support the framing of the entire discourse as a form of war. The immediacy created by drawing directly on the military register heightens the perceived severity of the events described.

(10) *Prosecutors and agents in the field are on the front lines confronting the cyber threats in their districts.* (S1)

Lexical items such as *front lines* and *confronting* suggest that the struggle is more akin to a physical battle than to legal proceedings. Despite the legal context, such language implies that a military response is warranted. Prosecutors and agents are cast as soldiers and combatants on the cyber battlefield. This evokes a sense of crisis and urgency while concomitantly portraying the actors as heroic defenders of community security. Cyber threats are metaphorically portrayed as challenges to be confronted, which dehumanises the adversaries and obscures the underlying causes of the attacks. The argument also spatialises the issue, with agents *in their districts* defending what is framed as territorial sovereignty against a perceived invasion. By discursively drawing *territorial borders* and claiming their transgression, rationale is provided for immediate and resolute action.

Director Keast-Butler exploits the military jargon in a similar vein:

(11) *We're working with partners to identify and disrupt criminals abroad; using our intelligence to prevent many millions of pounds of fraud here in the UK, and deploying cyber operations to remove child sexual abuse material. Together, we stand as a robust line of defence against the misuse of AI.* (S2)

She emphasises defence rather than deterrence and frames the threat as both imminent and indicative of a crisis. The pronouns *we* and *our* are exclusive and refer to the Government Communications Headquarters (GCHQ), the British intelligence agency where she serves as director. The adverb *together* is critical in implying collective responsibility and unity against an external enemy. The term *robust* is likely a deliberate exaggeration intended to reassure the audience of the state's strength and commitment. The spatial frame establishes a clear distinction between the negative representation of *wrongdoers* and the positive representation of *defenders*, in what is only half of Van Dijk's (1998) ideological square. Although Keast-Butler does not specify who the abusers of AI are, she reduces the issue to a simple good-versus-evil dichotomy to justify her calls for discipline and national unity.

The second semantic macrostructure demonstrates the strategic use of intertextuality to emphasise the significance of the cyber threat. It manifests through allusions to past terrorist attacks and ongoing conflicts.

(12) *Even as hundreds of individuals were convicted of terrorism or terrorism-related crimes in federal courts in the decade after 9/11, we knew that the measure of success was not a conviction but a stopped plot – the imperative to detect and disrupt a terrorist attack before it occurs. Today, there remains no greater priority for the Justice Department than international terrorism – as the horrific October 7th attacks remind us.* (S1)

David Newman references two significant events in the history of West-East conflicts. The September 11 attacks of 2001 constituted an Al-Qaeda-backed operation involving plane crashes that struck the World Trade Center in New York and the Pentagon, headquarters of the US Department of Defense (Office of the Secretary of Defense, n.d.). Another impactful event was the October 7 attack of 2023, in which a Hamas-led operation targeted Israel in the Gaza Strip, resulting in the deaths of 1,200 Israelis (US Department of State, 2024). The repercussions of this conflict are still unfolding and remain deeply relevant.

In describing the new regulatory framework of the NSD, David Newman further asserts:

(13) *The Department last summer established the National Security Cyber Section – or "Nat Sec Cyber" – within NSD. This new section – the first new enforcement section in NSD's history – puts cyber on an equal footing with counterterrorism and traditional counterespionage threats.* (S1)

Though not explicitly intertextual, such reasoning that echoes terrorist attacks is rhetorically powerful. While cybersecurity is framed within a criminal context throughout the speech, the turn to a response grounded in counterterrorism (example 13) reflects a recalibration of security which elevates cyber threats to matters of primary importance and tacitly likens cyber attackers to terrorists. The institutionalisation of the issue legitimises the NSD as a vigilant authority but resonates with the United States' *war on terror* era (2001-2021), when increased surveillance and data collection were not viewed as privacy infringements but as essential tools for ensuring national security. This portrayal reinforces the state's role as a protector and bolsters nationalistic sentiments. Russian discourse on cybersecurity adopts comparable strategies, with threats attributed to *foreign entities* and *international terrorist organisations*, said to undermine Russia's competitiveness in the information technology sector (Information Security Doctrine of the Russian Federation, 2000).

Senator Paterson mentions the war in Ukraine to argue that the uncontrolled development of new technologies, particularly AI, could lead to imminent danger (example 14). He views the disruptions occurring in cyberspace as harbingers of global conflict – one that, owing to the increasing sophistication of cyber capabilities, will become unrecognisable in its form and nature.

(14) *Russia's devastating war in Ukraine has dragged on for another year, and Ukraine's incredible resilience in fighting a hybrid war has been instructive on the importance of public-private partnership for national security and the nature of cyber warfare in the modern era.* (S3)

In this intertextual reference, Ukraine and Russia are personified, and a dichotomy between them along an axis of good versus evil is established. By employing the adjective *devastating*, Senator Paterson takes a strong stance against Russia and aligns himself with the West. He uses the verb *drag* (a material process) and the determiner *another* to illustrate the scope and longevity of the war. The term *hybrid war*, emphasises the critical importance of cyber defence and suggests that traditional military training is inadequate in addressing the complexities of modern conflict. He attributes Ukraine's resilience to a cooperation between public and private sectors, though the private institutions involved remain unidentified. This idea is supported in S1 and expanded upon in the fourth macrostructure.

The third semantic macrostructure is grounded in expressions of Western agency, particularly with regard to the United States. In contrast to their adversaries, the West is portrayed as operating transparently and decisively within a robust legislative framework.

(15) *While we always look to make arrests where possible, our law enforcement disruptions can take many forms. That's a matter of necessity because*

> *many of our investigative cyber targets — particularly in the national security and ransomware space — are protected by hostile governments such as Russia and Iran. In some cases, we know they receive such protection in exchange for being "on call" for their local military or intelligence services. So how is law enforcement disrupting actors outside the context of criminal charges and arrests? Most prominently, we are emphasizing court-authorized technical operations to, at scale, curtail and even, at times, eradicate the infrastructure these bad actors are using against us.* (S1)

The exclusive pronouns *we*, *our* and *us* strengthen a sense of unity within the NSD, while phrases like *make arrests* or *court-authorized technical operations* imply legality. The noun phrases *law enforcement*, *investigative cyber targets* and *technical operations* dampen emotions in favour of formality yet remain vague and leave the audience questioning the nature of these operations and the criteria for court approval. Such phrasing nonetheless lends an air of reliability to the NSD.

A rhetorical question is posed to create momentum, while human agency is attributed to *law enforcement*, rather than the actors behind these operations. By incorporating the prepositional phrases *at scale* and *at times*, Newman presents the United States as measured and temperate in its cyber responses. The evaluative adjectives *hostile* and *bad*, along with the prepositional phrase *against us*, function as polarising devices that amplify the emotional weight of the utterance. By listing Iran and Russia, one infers they are the intended *bad actors*, though the prepositional phrase *such as* suggests the implication of a broader group. The present continuous tense highlights the fluidity of events in cyberspace, while the two key material processes the US seeks to carry out – *curtail* and *eradicate* – imply finality and project a future triumph over their *advancing* adversaries.

While remaining within the bounds of the legal framework, Newman continues to assert:

> (16) *Using one of our age-old investigative tools, a Rule 41 search and seizure warrant, we deleted Volt Typhoon's malware and took steps to sever the routers from the botnet.* (S1)

He consistently employs the exclusive *we* to fully align himself with the National Security Department and cultivate a sense of collective agency within the institution. The richly modified noun phrase *age-old investigative tools* casts the NSD as experienced and trustworthy, while the metaphorical use of *tools* to denote search and seizure warrants functions as a strategic understatement. Referencing Rule 41[7]

[7] Rule 41 of the Federal Rules of Criminal Procedure outlines the procedures for obtaining warrants to conduct searches and seizures.

further reinforces the NSD's commitment to established legal procedures and effectively legitimises its actions. The verbs *delete* and *sever* indicate material processes and convey a decisive, proactive form of intervention. By contrast, the conventional metaphor *took steps* conceptualises the response as incremental and signals the complexity of an operation that unfolds through multiple stages. The phrasing also serves to hedge the statement and subtly mitigate responsibility, as it leaves ambiguous whether the routers will ultimately be successfully severed. What remains clear, however, is the adversarial relationship constructed between the NSD and the Chinese state-sponsored hacker group Volt Typhoon. While *malware* (short for malicious software) technically refers only to the software, the tone of the speech extends its negative connotations to both the group and the state backing it.

Rather than directly naming adversaries or their affiliated groups, Senator Paterson (example 17) and Director Keast-Butler (example 18) employ the familiar yet vague metonymic contrast between *the right* and *the wrong* hands. In doing so they effectively enact Van Dijk's (1998) ideological square with respect to positive self-representation and negative other-representation.

(17) *This underscores that, in the right hands, these new technologies can provide an asymmetrical advantage against those who would seek to do us harm.* (S3)

(18) *We need to protect our sensitive data from falling into the wrong hands.* (S2)

The emotional appeal of the fixed phrase generates anxiety and evokes a sense of urgency. While the speeches do not explicitly indicate whose hands are considered right or wrong, they provide sufficient evidence to suggest that a West/East dichotomy is being redrawn. According to Senator Paterson's reasoning, if the West was to gain control over emerging technologies, it would ensure their ethical use. In contrast, the blacklisted countries, if given the same privileges, would supposedly exploit these technologies for unethical and harmful purposes. Director Keast-Butler establishes a sense of collective identity by employing the inclusive pronoun *we* and the semi-modal verb *need* to imply a shared responsibility among the community. Her pressing need for security is further emphasised by the adjective *sensitive*, which underscores the value and the vulnerability of personal data.

Regarding the fourth semantic macrostructure, all three speeches underscored the significance of international partnerships and public-private cohesion, although differences in power dynamics among the nations did emerge.

(19) *It deserves emphasizing that this is a team sport: Even as the operations relied on Justice Department legal process, we are often not alone in planning or executing them. We are almost always joined by a coalition of US*

> *government, private sector, and foreign partners in this work. In disrupting the GRU botnet, for example, we planned and coordinated with the Shadowserver Foundation, Microsoft, and other private sector partners. Shortly after we announced the operation, the FBI, NSA, Cyber Command, and 11 foreign partner entities released a joint cybersecurity advisory providing device owners and network defenders with valuable threat intelligence about the GRU's relevant tactics, techniques, and procedures*. (S1)

The *team sport* metaphor in Newman's speech implies collaboration and shared responsibility within the NSD. Yet the narrative soon re-militarises, with lexical items such as *operations*, *executing*, *coalition*, *disruption* and *tactics*. This overlap is unsurprising, as notions of war and combat frequently find expression in sports terminology (Raffaelli & Katunar, 2016; Zerrad & Boujghagh, 2025). The verbs *plan* and *coordinate* (mental processes) portray the NSD's efforts as well thought out and deliberate, while the reference to the GRU, Russia's prominent intelligence agency, reinforces a polarisation along US-Russia lines.

Furthermore, Newman presents private institutions as *partners*, although he fails to elaborate on the nature or scope of their involvement. He lists the Shadowserver Foundation, a non-profit security organisation devoted to improving internet security (The Shadowserver Foundation, n.d.) and Microsoft. This highlights the fluid boundaries between public and private sectors, as well as the influence technology companies have on governmental policy. *11 foreign partners* are also referenced to indicate the importance of extending these efforts beyond US borders, yet no clarity is provided as to who they are or whether they operate publicly or privately. Praising private partners and companies for their role in cybersecurity suggests that the US is increasingly reliant on private capital and resources to combat cybercrime. Such collaboration also raises concerns about government intelligence agencies gaining access to personal user data, as well as a cybersecurity narrative that stretches beyond foreign threats and into citizens' private lives.

Director Keast-Butler also underscores the importance of private businesses in combating cyber threats on an international scale and implies that cybersecurity transcends national borders.

> (20) *In a moment you'll hear from Harry Coker, US Cyber Director, and Heather Adkins, Head of Google's Office of Cybersecurity Resilience. Just two fantastic speakers that showcase the importance of collaboration with business, and the strength of our international partnerships. Our partnerships are our competitive edge.* (S2)

The credibility of the two US representatives is anchored in their leadership roles – one as a *director* of a state agency and the other as a *head* in the private sector – as

well as in their supposedly *fantastic* oratory skills. This evaluative framing shapes audience expectations, while the direct address *you'll* and the inclusive pronoun *our* both engage listeners and foster a sense of collective identity. Together, these choices work persuasively to reassure the UK public of the critical role the US plays in supporting their cybersecurity efforts.

On the other hand, Newman adopted a philanthropic stance and positioned the US as self-sufficient but willing to assist weaker foreign governments:

(21) *We also use the criminal justice system to identify and attribute malicious activity – and to impose consequences on actors who may be specifically deterred even when foreign governments cannot.* (S1)

The exclusive *we* bespeaks the collective authority of the NSD's administration and positions the speaker as a representative of a powerful institution. Again, alignment with the criminal justice system and a stated commitment to deterrence further strengthen these claims to legitimacy. The term *malicious activity* is vague and leaves ample room for interpretation. Rather than defining what counts as harmful behaviour, the discourse leaves decisions about criminalisation to the Justice Department's discretion. The supposed inability of *foreign governments* to address cyber threats is signalled through epistemic modality, and in turn reinforces US dominance in cybersecurity.

This is echoed in both Australia and the UK, where explicit appeals are made for international partnerships. For instance, Senator Paterson highlights the need to follow the US in its efforts to curb cybercrime.

(22) *FBI Director Christopher Wray told the US Congress in January that "The PRC has a bigger hacking program than every other major nation combined. In fact, if each one of the FBI's cyber agents and intelligence analysts focused exclusively on the China threat, China's hackers would still outnumber FBI cyber personnel by at least 50 to 1." If that is true of a country like the United States, it's fair to say Australia isn't going to win a numbers game. This is why we need to work with our allies to accelerate technological innovation and embrace new technologies that can give us an edge in the cyber domain.* (S3)

He appeals to reason through statistics, while his argument gains credibility by citing an FBI representative. With the inclusive use of *we*, he fosters a sense of collective responsibility, and by invoking the material process of acceleration, he underscores urgency and delivers a call for international collaboration. The US is referred to as an ally, but the other partners remain unspecified. With a notably defeatist tone, the senator concedes Australia's subordinate position within the cybersecurity landscape and presents these alliances as a necessity rather than a choice.

The US, however, does not explicitly reference the UK or Australia (or their alliances), but instead maintains a level of ambiguity by broadly referring to *foreign partners* and *other foreign victims*. This interplay raises the question of whether their domestic concerns over cybersecurity merely reflect the broader US-China and US-Russia dichotomies. While the relationships between Western nations are construed as genuine friendships grounded in a shared commitment to democratic ideals, one is left to wonder whether the rhetoric of solidarity would persist in the absence of perceived competition for global influence.

6. The Common Culprits: Attribution in Cyberspace

As noted in the previous section, the actors behind the referenced cyber-attacks were effectively villainised and framed as enemies. It was suggested that the true orchestrators operate behind the scenes yet remain omnipresent. Table 2 lists the supposed perpetrators, as identified in the analysed speeches. It includes references to entire nation-states and specific individuals. In some cases, the attributions were phrased ambiguously, leaving it to the reader to interpret who the speaker was accusing of violating cyber laws.

Table 2 Cyber attribution across the three speeches

Identified attackers	**S1**	**S2**	**S3**
Nation-states	People's Republic of China (PRC) and its state-sponsored hackers known as "Volt Typhoon"	People's Republic of China (PRC)	People's Republic of China (PRC) state-sponsored cyber actors
	Russia and the Russian GRU	Russian intelligence services and proxy groups	Russia
	Iran and Iranian-backed proxies	Iran	Iran
	The Democratic People's Republic of Korea (DPRK)	North Korea	North Korea
Specific individuals	an employee at Apple working for a subsidiary of a Chinese company	leader of the LockBit ransomware group	Aleksandr Ermakov
	a software engineer at Google	Russian national Dmitry Khoroshev.	Russian hackers
Vaguely phrased attributions	international terrorist groups	hostile actors fraudsters criminals abroad	our adversaries
	authoritarian governments	nation-states	at least one foreign country one nation-state

The table identifies China, Russia, Iran, and North Korea as the primary nation-states behind the cyber-attacks. By explicitly blaming these countries and framing their actions as part of a coordinated effort, the discourse intensifies the severity of the attacks. Even when individuals such as *an employee at Apple working for a subsidiary of a Chinese company* or *Russian national Dmitry Khoroshev* are mentioned, pre- and post- modifiers define them primarily in terms of their nationality. This reduction enables their scapegoating and allows such accusations to divert attention from flaws in domestic security systems. With the villains so clearly defined, the narrative becomes easy to consume and accept.

The actions of these four enemy countries thus justify the need for retaliatory Western partnerships. Using the nations' full names and respective acronyms adds formality and a sense of *otherness*, while phrases such as *state-sponsored hackers* or *proxies* attach explicit political labels to the events occurring in cyberspace. The first two dimensions of Van Dijk's (1998) ideological square are reinforced, with a positive representation of *us* and a negative representation of *them*. However, the square is not fully realised, as China is portrayed positively in terms of the economic benefits obtainable from their cooperation with the UK:

(23) *Russia and Iran pose immediate threats, but China is the 'epoch-defining' challenge. The people of China and the Chinese community overseas have contributed greatly to life here in the UK. But recent events remind us that our country and democratic institutions remain of interest to the Chinese authorities. We want to engage with China where it's mutually beneficial.* (S2)

Director Keast-Butler ranks the *threatening* nation-states based on their potential to inflict harm. The adjective *immediate* contrasts with and is diluted by the modifier *epoch-defining*, which suggests that China's influence is subtler, but could ultimately culminate in significant disruption. This contrasts Russia and Iran, whose threats, though concerning, are less insidious. The subtlety attributed to China is linked to the narrative surrounding Chinese migration to the UK. Although articulated in a positive light, it is cautioned as a potential gateway for covert Chinese interference. Allusions to subversion and authoritarianism subtly reassert the boundaries that may have blurred between China and the UK. By invoking democratic institutions, Director Keast-Butler frames cybercrime as more than a security concern and elevates it to an issue of sovereignty and ideology. Her tone conveys a high level of certainty, but the use of complex sentence structures enables nuanced reflections on the multifaceted UK-China relationship. While the Chinese authorities are distinguished from the *people of China*, this phrase nonetheless subtly reinforces notions of possession and obedience. Dramatic tension is heightened by placing the key points last in a contrastive structure. The UK is portrayed as an

attractive target with valuable resources *of interest to* China. The use of the verb *want* (a mental process) tactfully implies that the UK's economic partnerships are a matter of choice rather than necessity, a perspective that is, in reality, flawed.

A notable specificity of cybercrime highlighted in the speeches aligns with Cavelty's (2013) observation that cyber threats do not originate from a single external source but are embedded within highly unpredictable network systems. This ambiguity is reflected in broad nationalised and politicised attributions, as seen in the following example that links the threat to the Chinese Communist Party. The risks are presented as multilayered, with these actors having the capacity to access the personal data of ordinary citizens just as easily as they can infiltrate large-scale infrastructure.

(24) *This means the CCP can use TikTok to access the data of millions of Australians, and can put its thumb on the scale of the TikTok algorithm to push China's preferred narratives to actively influence its users.* (S3)

Senator Paterson suggests that the Chinese government wields significant influence over Australian citizens. The statement's epistemic modality conveys moderate plausibility, while still allowing enough rhetorical leeway to persuade the public of the need for immediate action. The idiomatic expression of *the thumb being put on the scale* is central to framing the CCP's agenda as deceptive and manipulative. It draws on a commercial metaphor to simplify the issue and make it more relatable, especially for younger audiences who are the primary users of TikTok.

Foreign nation-states were not the only actors set on disrupting the digital environment. Technology itself, particularly generative AI, was personified and portrayed as a harbinger of future danger.

(25) *AI will heighten the global ransomware threat and increase the volume and impact of cyberattacks in the next two years.* (S3)

Senator Paterson's remarks speak to emerging vulnerabilities driven by rapid technological change. Such anxieties are not entirely new; as Beck (2009) argues in his theory of the global risk society, technological advances that enable sophisticated risk mitigation have, in fact, generated a pervasive sense of fear and reflexivity. Global communities are haunted by risks that, though neither seen nor felt, still permeate the collective consciousness (p. 8). This climate of uncertainty is discursively constructed across the speeches and creates fertile ground for antagonistic narratives to take root and further entrench existing geopolitical divisions.

JEZIKOSLOVLJE
27.1 (2026): 289-313

7. Conclusion

This research aimed to uncover the ideological underpinnings of public discourse on cybersecurity across three Western contexts: the US, the UK, and Australia. The research focused on global semantic structures, intertextuality, and the linguistic representation of both *attackers* and *victims*. Global propositions centred on future threats that were discursively constructed to legitimise preventive action. Retaliatory measures were accordingly legalised and framed as part of a supposed battle against an invisible authoritarian regime operating within network systems.

Progressive forms, emotionally charged intensifiers, and figures of speech were employed to enhance the memorability and persuasive force of the discourse. The speakers closely aligned themselves with their respective institutions and consistently used both exclusive and inclusive collective pronouns to build credibility and, respectively, invoke a sense of shared responsibility. The overall atmosphere was one of urgency with clear and insistent calls to action. Frequent military borrowings contributed to the construction of a cyberwar narrative that was framed as a defensive effort, with no explicit acknowledgement of the West's own ambition to secure strategic advantage in cyberspace.

Intertextual references to past terrorist attacks, namely 9/11 and the October 7th, as well as ongoing conflicts, were invoked to emphasise the importance of national security and international partnerships. Unlike the US, both British and Australian speakers voiced their national vulnerabilities, but believed these could be addressed through international cooperation. Internal cohesion and unwavering trust in government institutions were deemed sufficient in the US. Yet, the US did present itself as willing to selflessly share its resources with the *less capable* democratic world. Such claims warrant critical scrutiny, given that history repeatedly shows how larger power struggles are often pursued through minor alliances.

The three nations proved largely homogenous in their attribution of cybercrime, with attackers consistently viewed through the prism of four nation-states: Russia, China, Iran and North Korea. This deliberate simplification served to deepen the divide and polarise the *benevolent* West from the *malicious* East. Similar rhetoric appears in Russian cybersecurity discourse, where legality is likewise given priority. This includes the development of a unified regulative framework that claims to protect individual freedoms while serving the broader struggle to preserve national sovereignty (Information Security Doctrine of the Russian Federation, 2000). Such an entanglement of national and private interests provokes both personal anxieties and state-driven responses, which in turn allow calls to action to resonate across micro and macro levels. Ultimately, the findings of this research reinforce Cavelty's (2013) view of discursive realms as competitive arenas where stakeholders vie to assert their own versions of truth. While this analysis has revealed the extent to which

cybersecurity is ripe for such contests, the challenge of reconciling these self-victimising, war-inflected narratives clearly exceeds the boundaries of this study and remains a pressing task for future research.

References

Anderson, C., & Sadjadpour, K. (2018). Iran: Target and Perpetrator. In *Iran's Cyber Threat: Espionage, Sabotage, And Revenge* (pp. 9–16). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep26913.8

AUKUS: A Commitment to the Future. (2023). United States Department of State. https://www.state.gov/aukus-a-commitment-to-the-future/

Beck, U. (2009). *World at risk*. Polity.

Bey, M. (2018). Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition. *The Cyber Defense Review*, 3(3), 31–36. https://www.jstor.org/stable/26554994

Boo, H. (2017). An Assessment of North Korean Cyber Threats. *The Journal of East Asian Affairs*, *31*(1), 97–117. http://www.jstor.org/stable/44321274

Cavelty, M. D. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122. http://www.jstor.org/stable/24033170

Clarke, R. A., & Knake, R. K. (2014). *Cyber war*. Tantor Media, Incorporated.

Duyvesteyn, I. (2014). Between doomsday and dismissal: Cyber war, the parameters of war, and collective defense. *Atlantisch Perspectief*, *38*(7), 20–24. https://www.jstor.org/stable/48581164

Fairclough, N. (1992). Discourse and text: Linguistic and intertextual analysis within discourse analysis. *Discourse & society*, *3*(2), 193–217.

Fairclough, N. (2005). Critical discourse analysis in transdisciplinary research. *A new agenda in (critical) discourse analysis*, 13, 53–70.

Fairclough, N. (2010). *Critical discourse analysis: The critical study of language* (2nd ed.). Routledge.

Fairclough, N. (2013a). *Language and power*. Routledge.

Fairclough, N. (2013b). Critical discourse analysis. In *The Routledge handbook of discourse analysis* (pp. 9–20). Routledge.

Fairclough, N., & Wodak, R. (1997). Critical discourse analysis. In T. A. van Dijk (Ed.), *Discourse studies: A multidisciplinary introduction* (Vol. 2, pp. 258–284). Sage.

Fidler, D. P., Pregent, R., & Vandurme, A. (2013). NATO, Cyber defense, and international law. *St. John's Journal of International & Comparative Law*, *4*, 1–25. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub

Five Eyes accustomed to fabricating, spreading lies about China: Chinese FM - Global Times. (2023). Globaltimes.cn. https://www.globaltimes.cn/page/202310/1300391.shtml

Fung, C. J. (2022). China's use of rhetorical adaptation in development of a global cyber order: a case study of the norm of the protection of the public core of the internet. *Journal of Cyber Policy*, *7*(3), 256–274. https://doi.org/10.1080/23738871.2023.2178946

Granwal, L. (2023, September 20). *Australia: leading iron ore export destinations 2020*. Statista. https://www.statista.com/statistics/1149300/australia-leading-iron-ore-export-destinations/

Hausmann, R., Schetter, U., & Yildirim, M. A. (2024). On the design of effective sanctions: The case of bans on exports to Russia. *Economic Policy*, *39*(117), 109–153. https://doi.org/10.1093/epolic/eiad043

Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine*. NATO Defense College. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=124343&lng=en

Information Security Doctrine of the Russian Federation. (2000). International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Kanik, R. (2011). *Internet Governance in an Age of Cyber Insecurity*. Council on Foreign Relations. https://cdn.cfr.org/sites/default/files/pdf/2010/08/Cybersecurity_CSR56.pdf

Mahmoud, K. W. (2013). *Cyber Attacks: The Electronic Battlefield*. Arab Center for Research & Policy Studies. http://www.jstor.org/stable/resrep12651

Mauro, A. (2024). *The language of cyber attacks: A rhetoric of deception*. Bloomsbury Publishing.

Nagy, V. (2012). The geostrategic struggle in cyberspace between the United States, China, and Russia. *AARMS: Academic & Applied Research in Military Science*, *11*(1), 13–26.

Office of the Secretary of Defense. (n.d.). *9/11 attack*. US Department of Defense. https://history.defense.gov/DOD-History/Pentagon/9-11-Attack/

Office of the United States Trade Representative. (2023). *The People's Republic of China | United States Trade Representative*. Ustr.gov; Office of the United States Trade Representative. https://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china

Pigman, L. (2019). Russia's vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion. *Journal of Cyber Policy*, *4*(1), 22–34. https://doi.org/10.1080/23738871.2018.1546884

Raffaelli, I., & Katunar, D. (2016). A Discourse Approach to Conceptual Metaphors: A Corpus-Based Analysis of Sports Discourse in Croatian. *Studia Linguistica Universitatis Iagellonicae Cracoviensis*, *133*(2), 125–147. https://doi.org/10.4467/20834624SL.16.010.5156

Ramirez, R., & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: a literature review. *IEEE Access*, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rugge, F. (2018). An 'axis' reloaded? In Rugge, F. (Ed.), *Confronting an 'axis of cyber'? China, Iran, North Korea, Russia in cyberspace* (pp. 13–37). Ledizioni LediPublishing.

Simons, G., Manoilo, A. V., & Goncharenko, A. R. (2024). Projecting "hybrid warfare": Western discursive representation of Chinese foreign policy. *Vestnik RUDN International Relations*, *24*(3), 345–357. https://doi.org/10.22363/2313-0660-2024-24-3-345-357

The Shadowserver Foundation. (n.d.). *The Shadowserver Foundation*. https://www.shadowserver.org

US Department of State. (2024, October 7). *Anniversary of October 7th attack*. https://www.state.gov/anniversary-of-october-7th-attack/

Van Dijk, T. A. (1976). Narrative macro-structures. *PTL: A journal for descriptive poetics and theory of literature, 1*, 547–568.

Van Dijk, T. A. (1980). *Macrostructures: An interdisciplinary study of global structures in discourse, interaction, and cognition*. Lawrence Erlbaum Associates.

Van Dijk, T. A. (1998). *Ideology: A Multidisciplinary Approach*. Sage.

Van Dijk, T. A. (2001). Critical discourse analysis. In D. Tannen, D. Schiffrin, & H. Hamilton (Eds.), *Handbook of discourse analysis* (pp. 352–371). Blackwell.

Van Dijk, T. A. (2005). Discourse analysis as ideology analysis. In C. Schäffner and A. Wenden (Eds.), *Language and Peace* (pp. 41–58). Routledge.

Van Dijk, T. A. (2011a). Discourse studies and hermeneutics. *Discourse Studies*, 13(5), 609–621. http://www.jstor.org/stable/24049952

Van Dijk, T. A. (2011b). Discourse and ideology. *Discourse studies: A multidisciplinary introduction*, 2, 379–407.

Van Epps, G. (2013). Common ground: US and NATO engagement with Russia in the cyber domain. *Connections*, *12*(4), 15–50.

Wodak, R. (2001). The discourse-historical approach. *Methods of critical discourse analysis*, 1, 63–94.

Wodak, R. (2014). Critical discourse analysis. In C. Leung & B. V. Street (Eds.), *The Routledge companion to English studies* (pp. 302–316). Routledge.

Zerrad, E. M., & Boujghagh, H. (2025). Between sport and war: exploration of military terminology in the Moroccan and French sports press. *International Journal of Scientific Research and Innovative Studies*, *4*(5), 56–61. https://doi.org/10.63883/ijsrisjournal.v4i5.455

Zhou, F. (2023). China-Australia Relations and China's Policy Choices toward Australia: A Chinese Perspective. *China Review*, *23*(1), 213–242. https://www.jstor.org/stable/48717994

Analysed Speeches

Keast-Butler, A. (2024). *CYBERUK 2024: Anne Keast-Butler keynote speech. (2024). Ncsc.gov.uk. https://www.ncsc.gov.uk/speech/cyberuk-2024-gchq-director-keynote-speech*

Newman, D. (2024). *Principal Deputy Assistant Attorney General David Newman Delivers Remarks at 2024 U.S. Cyber Command Legal Conference*. (2024, April 17). Justice.gov. https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-david-newman-delivers-remarks-2024-us-cyber

Paterson, J. (2024). *Transcript | Speech to the AISA Canberra Australian Cyber Conference | 27 March 2024*. (2024). Senatorpaterson.com.au. https://www.senatorpaterson.com.au/news/transcript-speech-to-the-aisa-canberra-australian-cyber-conference-27-march-2024

JEZIKOSLOVLJE
27.1 (2026): 289-313

DISKURS KIBERNETIČKE SIGURNOSTI: KRITIČKA ANALIZA ZAPADNIH PREDODŽBI O KIBERNETIČKIM PRIJETNJAMA

U ovom radu analiziraju se jezični obrasci u unutar diskursa o kibernetičkoj sigurnosti. Riječ je o fenomenu koji u političkom diskursu sve više prožima ideologija, često nauštrb načela objektivnosti i točnosti. Istraživanje donosi kritičku analizu triju govora vladinih dužnosnika iz Sjedinjenih Država, Ujedinjenog Kraljevstva i Australije. Poštujući metodološka načela kritičke analize diskursa, istraživanje se oslanja na Van Dijkove koncepte lokalnih i globalnih značenja, Wodakov i Faircloughov pristup intertekstualnosti te Van Dijkov ideološki kvadrat. Rezultati pokazuju da zapadne sile smještanjem kibernetičke sigurnosti u kriminalni kontekst zauzimaju ulogu arbitara pravde. Prijetnje kibernetičkoj sigurnosti prikazuju se kao trajne i neposredne, a naglašavaju se nesvršenim oblicima i emocionalno nabijenim frazama. Analiza intertekstualnosti otkriva oslanjanje na prošle terorističke incidente i aktualne geopolitičke sukobe s ciljem izazivanja straha i potpirivanja animoziteta prema određenim društvenim skupinama. Istraživanje također ukazuje na problematičnu upotrebu vojne terminologije, unatoč odsutnosti stvarnog rata u kibernetičkom prostoru. Nacionalne države personificirane su kao krivci, a kibernetički napadi prikazuju se kao manifestacije njihove težnje prema potkopavanju demokracije i nametanju globalne dominacije. Navedene diskurzivne prakse provociraju kritičku misao te upozoravaju na postojanu polarizaciju Zapada i Istoka kao odraz dugotrajnih podjela u fizičkom svijetu. Kako ovaj diskurs oblikuje naše razumijevanje stvarnosti, takve podjele mogu pretvoriti zamišljene prijetnje u samoispunjavajuća proročanstva. Stoga je nužno osigurati terminološku preciznost i pojmovnu jasnoću kako bi se prepoznao i suzbio manipulativni potencijal diskursa o kibernetičkoj sigurnosti.

Ključne riječi: kibernetička sigurnost, kritička analiza diskursa, ideologija, globalno značenje, lokalno značenje, intertekstualnost

Adresa autorice:

Adriana Petra Blažević
Filozofski fakultet
HR – 21 000 Split, Poljička cesta 35
ablazevic1@ffst.hr