SILENT SKIRMISHES: CYBER WARFARE'S EROSION OF WESTPHALIAN PRINCIPLES IN THE PRELUDE TO THE 2022 RUSSIAN-UKRAINIAN WAR

ESCARAMUÇAS SILENCIOSAS: A EROSÃO DOS PRINCÍPIOS OCIDENTAIS PELA GUERRA CIBERNÉTICA NO PRELÚDIO DA GUERRA RUSSO-UCRANIANA DE 2022

DOI: 10.56083/RCV3N9-001
Recibimento do original: 28/07/2023
Aceitação para publicação: 29/08/2023

João Marcos Barbosa Oliveira
Specialist in Information Security Management
Institution: Escola de Aperfeiçoamento de Oficiais
Address: Avenida Duque de Caxias, 2071, Deodoro, Rio de Janeiro – RJ, CEP: 21615-220
E-mail: barbosaoliveira.joao@eb.mil.br

Eduardo Stefani
PhD Student in Informatics and Knowledge Management
Institution: Universidade Nove de Julho (UNINOVE)
Address: Rua Vergueiro, 235/249, Liberdade, São Paulo – SP, CEP: 01525-000
E-mail: eduardo_stefani@uni9.edu.br

Ivanir Costa
Doctor of Production Engineering
Institution: Universidade Nove de Julho (UNINOVE)
Address: Rua Vergueiro, 235/249, Liberdade, São Paulo – SP, CEP: 01525-000
E-mail: ivanirc@uni9.edu.br

ABSTRACT: The research explored the relationship between the Treaty of Westphalia’s principles of national sovereignty and non-intervention and Cyber warfare in the modern era, using the Russian-Ukrainian war as a case study. Through a literature review, the study examined how these principles are evolving in today's boundary-less digital world. An in-depth analysis of incidents between Russia and Ukraine from January 2020 to January 2022 revealed that both countries experienced significant cyber attacks. However, there was no evidence linking Ukraine to any incidents against Russia, and
no surge in incidents was observed prior to the events in Ukraine in February 2022. The study concluded that digital incidents appear did not significantly impact the Treaty of Westphalia’s principles, suggesting that these principles remain robust in the face of cyber challenges.

**KEYWORDS:** Cyberwarfare, Treaty of Westphalia, Russian-Ukrainian War.

**RESUMO:** A pesquisa explorou a relação entre os princípios do Tratado de Vestfália de soberania nacional e não-intervenção e guerra cibernética na era moderna, usando a guerra russo-ucraniana como um estudo de caso. Através de uma revisão da literatura, o estudo examinou como esses princípios estão evoluindo no mundo digital sem fronteiras de hoje. Uma análise aprofundada dos incidentes entre a Rússia e a Ucrânia de janeiro de 2020 a janeiro de 2022 revelou que ambos os países sofreram ataques cibernéticos significativos. No entanto, não havia provas que ligassem a Ucrânia a quaisquer incidentes contra a Rússia, e não se observou qualquer aumento dos incidentes antes dos acontecimentos na Ucrânia em fevereiro de 2022. O estudo concluiu que os incidentes digitais parecem não ter um impacto significativo nos princípios do Tratado de Vestfália, sugerindo que estes princípios permanecem robustos face aos desafios cibernéticos.

**PALAVRAS-CHAVE:** Ciberguerra, Tratado de Vestfália, Guerra Russo-Ucraniana.

1. Introduction

The establishment of the Treaty of Westphalia in 1648 marked the consolidation of state sovereignty, territorial integrity, and non-intervention norms, shaping the cornerstone of modern international relations (Charlesworth & Chinkin, 2022). This treaty concluded the Thirty Years' War and the Eighty Years' War, aiming to restore stability and tranquility to a Europe punctured by political and religious disorder (Bechtold, 2023). Since then, numerous contemporary events and advancements have both upheld and challenged the principles of the Westphalian system. One notable
example is the rise of cyber warfare, which has emerged as a significant challenge to the Westphalian principles (Broeders, 2017). Additionally, other factors such as globalization, transnational terrorism, and the increasing interconnectedness of nations have also posed challenges to the traditional Westphalian model.

Cyber warfare – the employment of digital technologies in offensive or defensive activities in cyberspace – has become an integral part of contemporary military strategies (Rid & McBurney, 2012). Both state and non-state actors' growing dependency on digital infrastructure and sophisticated cyber capabilities has transformed cyberspace into a theater for conflicts (Smeets, 2018). Nonetheless, the global reach of cyberspace and the anonymity inherent to cyber warfare present unique hurdles to traditional Westphalian principles (Lanoszka, 2016).

Territorial integrity and non-intervention principles face challenges due to the fading borders between states in cyber warfare (Lanoszka, 2016). Cyberattacks, originating from any global location and impacting multiple jurisdictions, make identifying perpetrators or enforcing Westphalian principles complex (Lanoszka, 2016). Furthermore, non-state actors' participation in cyber warfare interrupts the state-centric Westphalian system, as these groups can execute intricate cyber operations with substantial geopolitical repercussions (Bourne, 2018).

Over the past decade, numerous high-profile cyber incidents have revealed the Westphalian system’s susceptibilities to the global and anonymous facets of cyber warfare, culminating in a gradual disintegration of traditional geopolitical boundaries and norms (Adamson, 2016).

The 2008 cyberattack on Georgia, allegedly led by Russia, signified a turning point in cyber warfare history (Lalman, 2023). This event marked one of the initial occurrences of a state purportedly coordinating a large-scale cyber offensive against another, concurrent with a physical military invasion (Lalman, 2023). This coordinated cyber-physical attack blurred the lines of
state sovereignty and territorial integrity, displaying the potency of cyber warfare in geopolitical manipulation.

The unearthing of the Stuxnet worm in 2010 further highlighted the potential of cyber warfare to unsettle the Westphalian system (Choucri, Madnick, & Ferwerda, 2013). Widely ascribed to the United States and Israel, Stuxnet aimed to hamper Iran's nuclear program (Choucri, Madnick, & Ferwerda, 2013). This operation showcased the capacity of states to infringe upon others' sovereignty without a physical presence, posing a direct challenge to Westphalian principles of non-intervention and territorial integrity (Choucri, Madnick, & Ferwerda, 2013).

The persistent cyber conflict between Russia and Ukraine, escalating notably in 2014, has magnified these challenges (Browning, 2018). A sequence of cyberattacks, imputed to Russian state-sponsored actors, targeted vital Ukrainian infrastructure, causing extensive disruptions and showing cyber warfare's capacity to violate states' sovereignty (Browning, 2018).

This paper seeks to comprehend cyber warfare's effect on the Westphalian system's principles. Attention will focus on the cyberattacks transpiring between January 2020 and January 2022, immediately preceding the Russian incursion into Ukraine. The selected period will be scrutinized to ascertain whether a spike in cyber hostility towards or from these nations occurred, thus challenging Westphalian concepts of state sovereignty and non-intervention. The objective is to discern whether a rise in cyberattacks correlates with challenges to the Westphalian system's principles, even lacking physical incursion.

The approach entails analyzing the sequence of cyberattacks within this timeframe, considering each incident's nature, origin, and effect. This analysis will facilitate the evaluation of the extent to which cyber warfare questions the principles of the Westphalian system.
The study's outcomes could offer crucial insights into the evolving dynamics of international relations in the era of cyber warfare. It may illustrate how the Westphalian system might need to adjust to maintain stability and peace in the digital age, where state sovereignty, territorial integrity, and non-intervention norms face increasing scrutiny.

2. Literature Review

This section explores the key concepts of this study, including the principles of sovereignty and non-intervention, their relevance today, and the challenges posed by cyber warfare. It also examines important literature and theories in international relations that shed light on state interactions in the digital age. The aim of this section is to establish a basic understanding of how cyber warfare affects traditional global politics, setting the stage for a detailed analysis of the cyber conflict between Russia and Ukraine and its impact on the Westphalian system.

2.1 Treaty of Westphalia

The Treaty of Westphalia, a historical keystone in international relations, was concluded in 1648, marking the end of the Thirty Years' War and the Eighty Years' War (Charlesworth & Chinkin, 2022). A state-centric system was forged through these negotiations, which originated in 1644 and extended over four years, shaping global political structures for subsequent centuries (Bechtold, 2023; Hooghe & Marks, 2002). Delegates from diverse European powers assembled in two Westphalian cities, Münster and Osnabrück, to finalize this epoch-making diplomatic accord (Osiander, 2001).

The central principles of this Treaty, namely sovereignty and non-intervention, came to characterize the international state system (Osiander,
Recognition of the independent authority of over three hundred German states signaled a transition towards a system comprising co-existing sovereign states (Perkmann, 2007). Furthermore, the Treaty emphasized the importance of refraining from intervening in other states' domestic matters, thereby respecting their autonomy (Osiander, 2001; Perkmann, 2007).

Within the Westphalian framework, sovereignty refers to the complete control a state exercises over domestic affairs within its territorial boundaries, absent any foreign intervention (Elden, 2005; Acharya, 2014). Each state possesses exclusive authority over its territory, distinctly demarcating internal and external affairs (Elden, 2005; Acharya, 2014). This control aids in maintaining global order by discouraging unilateral actions that could instigate conflicts (Elden, 2005; Acharya, 2014). Nevertheless, this concept has undergone reinterpretation and evolution in response to changing global realities, such as the emergence of international organizations and growing state interconnection (Elden, 2005; Acharya, 2014).

Conversely, the principle of non-intervention centers on respect for the sovereignty of other states, dictating a norm against intervening in other states' internal affairs (Ayoob, 2002). This principle is not unalterable, with exceptions acknowledged under international law and the contentious norm of Responsibility to Protect (R2P) (Bellamy & Williams, 2011).

As the transition into the digital age progresses, territorial sovereignty, traditionally understood as absolute authority exercised within territorial borders, becomes increasingly indistinct in cyberspace (DeNardis, 2014). The borderless essence of the internet and digital technologies, alongside the challenge of attributing cyberattacks, undermines the principle of state sovereignty (Dunn Cavelty, 2014). Furthermore, the emergence of potent non-state actors, such as multinational tech corporations operating across national boundaries, confronts traditional notions of state control within their territories (Maurer, 2013).
In cyberspace, borders are determined by digital infrastructures and systems rather than geographic markers (Dunn Cavelty, 2014). The advent of cyber warfare presents novel challenges to this principle, as cyberattacks blur the boundary between domestic and international spheres (Lanoszka, 2016). Cyberattacks can originate from and target any global location, surpassing physical boundaries (Dunn Cavelty, 2014). Such realities problematize traditional conceptions of national defense and security, with states wrestling with threats that disregard their national borders (Maurer, 2013).

Additionally, the unimpeded flow of information in cyberspace and the storage, processing, and transmission of data across multiple jurisdictions have considerable implications for privacy, freedom of speech, and state control (Allen, 2011). In this digital, globalized world, non-state actors such as multinational corporations, international organizations, and cyber actors have surfaced as significant influencers, affecting state sovereignty and national borders (Amoore, 2011). Such actors, equipped with extensive resources and influence, can shape policy decisions and impact economies across borders, posing challenges to traditional sovereignty boundaries (Jiang & Fu, 2018).

In the digital world, non-state cyber actors can cause disruption to critical infrastructure, manipulate public opinion, or purloin sensitive information, with substantial repercussions for state sovereignty and security (Dunn Cavelty, 2014). The digital age continues to reshape and redefine the concepts of sovereignty and national borders (Mountz et al., 2013).

2.2 Cyber Warfare

As digital technologies and the internet become increasingly embedded in national infrastructure and shape society's dependence on technology, the nature and dynamics of conflicts have also transformed, leading to the
emergence of cyber warfare (Kello, 2013). Nevertheless, delineating cyber warfare presents complexity and remains a topic of extensive debate in academic and policy domains (Rid, 2012).

In essence, cyber warfare constitutes the execution of digital attacks by one state to impair another's computer systems, with the intention to inflict substantial damage, casualties, detriment, or sway outcomes (Kello, 2013). Cyber warfare can span an array of activities, from espionage, data theft, service disruption to physical infrastructure damage via digital pathways (Kello, 2013).

The sphere of cyber warfare extends beyond mere attacks inflicting physical harm or disruption, encompassing attempts aimed at impacting the integrity and availability of information (Kello, 2013). This extension reflects the information age's reality, where narrative control and perception shaping can be as pivotal as causing physical harm (Kello, 2013).

Regarding the actors involved, the scope of cyber warfare has widened beyond states to encompass non-state entities such as terrorist organizations, hacktivists, and criminal groups, thereby resulting in a more intricate and complicated cyber threat landscape (Sigholm, 2013).

Furthermore, cyber warfare's distinctiveness lies in its asymmetric nature (Tsagourias, 2012). In contrast to conventional warfare, in the cyber sphere, smaller states or even non-state actors can instigate significant attacks (Tsagourias, 2012). This situation blurs the combatant-civilian delineation and adds intricacy layers to international law's application (Tsagourias, 2012).

Cyberattacks involve activities intended to compromise the confidentiality, integrity, or availability of information systems (Kumar, 2011). Such attacks can target government entities, businesses, critical infrastructure, or individuals (Kumar, 2011). Cyberattack examples comprise malware infections, distributed denial-of-service (DDoS) attacks, and phishing (Kumar, 2011). Unauthorized access attainment, sensitive
information theft, operation disruption, or damage infliction often constitute cyberattacks' primary objectives (Kumar, 2011).

In the cybersecurity realm, comprehending key concepts underlying various cyber threats and attacks proves crucial. The ensuing table 1 offers a succinct overview of vital concepts, encompassing cyber intrusion, cyber operations, phishing campaigns, DDoS attacks, spearphishing, and malware attacks. Each concept signifies a distinct type of cyber threat, underscoring the diverse tactics and strategies utilized by adversaries in the digital landscape. By acquainting with these concepts, the nature and implications of cyber warfare can be better understood, enabling proactive system and information protection measures.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber intrusion</td>
<td>The unauthorized access or penetration of a computer system or network by an external entity for malicious purposes (Razzaq et al, 2013).</td>
</tr>
<tr>
<td>Cyber Operations</td>
<td>Coordinated activities conducted in cyberspace by individuals, organizations, or nations to achieve specific objectives, such as gathering intelligence, disrupting operations, or causing damage (Czosseck, Ottis &amp; Talihärm, 2007).</td>
</tr>
<tr>
<td>Phishing campaign</td>
<td>A systematic and targeted approach to deceive individuals or organizations into disclosing sensitive information, such as passwords or financial details, by masquerading as a trustworthy entity through fraudulent communication channels, typically emails or websites (Aburrous et al, 2010).</td>
</tr>
<tr>
<td>Malware attack</td>
<td>The deliberate deployment of malicious software, commonly referred to as malware, onto a system or network with the intent to compromise its security, steal data, or gain unauthorized access (Alazab et al, 2018).</td>
</tr>
<tr>
<td>DDoS attack</td>
<td>Distributed Denial-of-Service (DDoS) attack is a malicious attempt to overwhelm a targeted system or network with a flood of illegitimate traffic, rendering it unavailable to legitimate users (Wang &amp; Li, 2021).</td>
</tr>
<tr>
<td>Spearphishing attempts</td>
<td>A highly targeted form of phishing attack that involves personalized and tailored messages or communications aimed at specific individuals or groups to trick them into revealing sensitive information or executing malicious actions (Heartfield &amp; Loukas, 2018).</td>
</tr>
</tbody>
</table>

Source: Adapted from cited authors.
3. Methodology

The research conducted within this study utilizes a data-driven approach to assess cyber warfare's impact on Westphalian principles of sovereignty and non-intervention. The primary data source for this investigation is the "Significant Cyber Incidents" database, curated by the Center for Strategic & International Studies (CSIS). This database presents a thorough record of publicly disclosed cyberattacks globally, providing a robust and dependable tool for exploring the trend and repercussions of cyber warfare.

The selected time period for analysis, spanning January 2020 to January 2022, aligns with a phase of heightened geopolitical tensions between Russia and Ukraine, but notably concludes before the Russian military incursion into Ukraine. This time frame is chosen deliberately, not only for its contemporaneity but also because it provides a backdrop against which the trends and strategies in cyber warfare can be analyzed in light of escalating political discord.

Examining a recent conflict between two countries that has escalated into war provides a real-world context and immediacy that adds significant value to a research study. Current conflicts allow researchers to analyze contemporary strategies, tactics, and technologies in use, offering insights into the evolving nature of international relations and warfare.

Relevant data extraction from the CSIS database involved filtering entries to include solely incidents attributed to or targeted at Russian and Ukrainian entities. This methodology focused on the cyber activities of these two nations, yielding insights into their employment of cyber warfare amid escalating political discord.

Upon isolating pertinent data, a comprehensive analysis was conducted to discern trends, patterns, and significant incidents. This examination aimed to illuminate the influence of these cyber activities on Westphalian principles.
of sovereignty and non-intervention. More specifically, the inquiry sought to ascertain whether these cyberattacks violated these principles and, if they did, the mechanisms through which they did so.

4. Results and Discussion

The table 2 chronologically catalogs significant cyber incidents that transpired between January 2020 and January 2022, with a particular focus on cyberattacks targeted against Russia or Ukraine. The incidents are described in terms of the alleged attacker’s country, the targeted country, the nature of the cyberattack, and additional relevant details.

<table>
<thead>
<tr>
<th>Month/Year</th>
<th>Alleged attacker’s country</th>
<th>Country Targeted</th>
<th>Type of Attack</th>
<th>Other Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2020</td>
<td>Russia</td>
<td>Ukraine</td>
<td>Cyber intrusion</td>
<td>Infiltrated a Ukrainian energy company where Hunter Biden was previously a board member</td>
</tr>
<tr>
<td>July 2020</td>
<td>US</td>
<td>Russia</td>
<td>Authorized cyber operations</td>
<td>Included disruption and public leaking of information</td>
</tr>
<tr>
<td>July 2020</td>
<td>US</td>
<td>Russia</td>
<td>Operation by US Cyber Command</td>
<td>Took Russian Internet Research Agency offline</td>
</tr>
<tr>
<td>August 2020</td>
<td>Russia</td>
<td>Ukraine</td>
<td>Phishing campaign</td>
<td>Conducted in preparations for operations on Ukraine’s independence day</td>
</tr>
<tr>
<td>October 2020</td>
<td>North Korea</td>
<td>Russia</td>
<td>Cyber intrusion</td>
<td>Targeted aerospace and defense companies</td>
</tr>
<tr>
<td>October 2020</td>
<td>China</td>
<td>Russia</td>
<td>Multiple attacks</td>
<td>Details not specified</td>
</tr>
<tr>
<td>February 2021</td>
<td>Russia</td>
<td>Ukraine</td>
<td>Malware attack</td>
<td>Compromised a Ukrainian government file-sharing system</td>
</tr>
<tr>
<td>February 2021</td>
<td>Unknown</td>
<td>Ukraine</td>
<td>DDoS attack</td>
<td>Against the website of the Security Service of Ukraine</td>
</tr>
<tr>
<td>March 2021</td>
<td>Russia</td>
<td>Ukraine</td>
<td>Attempted cyber intrusion</td>
<td>Attempt to gain access to classified government data</td>
</tr>
<tr>
<td>April 2021</td>
<td>Russia</td>
<td>Ukraine</td>
<td>Spearphishing attempts</td>
<td>Targeted Ukrainian government officials</td>
</tr>
</tbody>
</table>
The provided timeline of cyberattacks from January 2020 to January 2022 illuminates the complexity and escalation of international cyber warfare activities, particularly involving Russia and Ukraine, while also showing global trends.

In January 2020, a notable cyber intrusion was executed by Russian actors against a Ukrainian energy company, demonstrating an early indication of the intense digital conflict between these nations. This trend of Russian-initiated attacks against Ukraine persists throughout the timeline, as exemplified in February and March 2021 with a malware attack and an attempted large-scale intrusion, respectively. In April 2021, Russian hackers also targeted Ukrainian government officials with spearphishing attempts, which is a classic cyber espionage tactic.

However, these attacks were not one-sided. As seen in the data, there were also significant digital attacks against Russia originating from different parts of the globe. Notably, in July 2021, an unknown actor launched a Distributed Denial of Service (DDoS) attack, causing a shutdown of the Russian defense ministry's website. Furthermore, in January 2022, a group

<table>
<thead>
<tr>
<th>Month/Year</th>
<th>Alleged attacker's country</th>
<th>Country Targeted</th>
<th>Type of Attack</th>
<th>Other Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2021</td>
<td>China</td>
<td>Russia</td>
<td>Cyber intrusion</td>
<td>Russian defense contractor involved in designing nuclear submarines compromised</td>
</tr>
<tr>
<td>June 2021</td>
<td>Unknown</td>
<td>Russia</td>
<td>DDoS attack</td>
<td>Vladimir Putin’s annual phone-in session was targeted</td>
</tr>
<tr>
<td>July 2021</td>
<td>Unknown</td>
<td>Russia</td>
<td>DDoS attack</td>
<td>Russian defense ministry’s website was shut down</td>
</tr>
<tr>
<td>January 2022</td>
<td>Unknown</td>
<td>Ukraine</td>
<td>Malware attack, Ransomware</td>
<td>Affected 90 government websites and damaged multiple computers in government agencies</td>
</tr>
<tr>
<td>January 2022</td>
<td>North Korea</td>
<td>Russia</td>
<td>Malware attack</td>
<td>Russian diplomats targeted via malicious email disguised as New Year greetings</td>
</tr>
</tbody>
</table>

Source: Adapted from Significant Cyber Incidents in Center for Strategic and International Studies (2023).
affiliated with the Democratic People's Republic of Korea (DPRK) used malware to target Russian diplomats.

Interestingly, there were also cyber activities initiated by nations beyond the primary Russia-Ukraine conflict. For example, Chinese and North Korean groups targeted Russia, and the United States authorized cyber operations against multiple countries, including Russia.

Overall, the timeline provides a stark picture of the ever-evolving landscape of cyber warfare, highlighting the increased threats to state sovereignty and underscoring the need for renewed understanding and strategies to handle these challenges within the framework of international relations. It is apparent that the Westphalian principles of state sovereignty and non-intervention are being severely tested in this digital era.

Delving deeper into this analysis, it is clear that the escalating cyber conflict, especially between Russia and Ukraine, is a reflection of the changing face of warfare and international relations. Cyber warfare creates a gray area in the traditional understanding of state conflict, as it often blurs the lines between military and civilian targets, state and non-state actors, and even borders themselves (Lanoszka, 2016).

One striking aspect revealed in the timeline is the diversity of attacks. From DDoS attacks and spearphishing attempts to cyber intrusions and the deployment of malware, these strategies demonstrate the versatility and severity of cyber warfare tactics. These varying methods not only have different levels of impact but also require different skills to both initiate and defend against them, demonstrating the need for evolving technological capabilities and sophisticated defenses in the international arena (Abomhara & Køien, 2015).

Furthermore, the difficulties associated with attributing cyberattacks also become evident. Many entries in the timeline list the initiating actor as "unknown" emphasizing the challenges in tracking the origins of these attacks. Attribution is critical in the sphere of international relations, as it
allows for the possibility of retaliation, sanction, or legal recourse. This attribution problem henceforth undermines traditional mechanisms of maintaining international order and respect for sovereignty (Henriksen, 2019).

The timeline also underscores the fact that cyber warfare is not confined to any one region or set of actors. It is truly a global issue, with countries like the United States, China, and North Korea also implicated in these activities. This global dimension implies that any comprehensive solution must involve international cooperation and multilateral discussions.

The data reveals an intriguing pattern concerning the prevalence of cyberattacks leading up to the Russian invasion of Ukraine in February 2022. Notably, there was no discernible escalation in the frequency or intensity of cyberattacks in the months immediately preceding the invasion. This contradicts any presumed correlation between an uptick in cyber warfare and impending physical conflict (Brunstetter & Braun, 2013).

Throughout 2020 and 2021, the regularity of cyberattacks involving Russia and Ukraine remained relatively stable, with incidents being distributed evenly over the two-year period. This indicates that the initiation of physical warfare was not preceded by a surge in cyber aggression, thus challenging the assumption that cyber warfare might serve as a bellwether for traditional warfare (Brunstetter & Braun, 2013).

Before the invasion in February 2022, there were cyberattacks targeting Ukrainian government websites and Russian diplomats in January 2022. However, these incidents were not significantly different from previous cyber events. Throughout 2021, there were various cyberattacks on government entities in both countries, but the frequency of these incidents did not notably increase leading up to the invasion. In fact, cyber incidents seemed to decrease slightly in the second half of 2021, indicating a relatively calm cyber landscape before the physical warfare.
This means that cyberattacks can continue even when things get worse in the real world. This means that cyber warfare might be more like a continuous war or a mix of wars instead of only getting worse before physical fights happen. The concepts of continuous war and hybrid wars represent a significant shift in the understanding of conflict. Continuous war refers to a state of ongoing, often low-intensity conflict, where warfare becomes a normal state of affairs (Bachmann & Mosquera, 2016). Hybrid wars, on the other hand, are characterized by the blending of traditional and non-traditional methods of warfare, involving both state and non-state actors (Bachmann & Mosquera, 2016). These wars can incorporate a range of tactics, including conventional warfare, irregular warfare, terrorism, and cyber warfare, typically simultaneously. The advent of hybrid wars has blurred the lines between peace and war, challenging traditional notions of conflict and necessitating a reevaluation of military doctrines and strategies.

Empirical evidence from the Russian-Ukrainian conflict challenges the notion that cyber warfare necessarily intensifies before a physical onslaught. This calls for a reevaluation of the interplay between cyber warfare, continuous warfare, and hybrid warfare models, necessitating a deeper exploration into the variables that affect the intensity and frequency of cyberattacks amidst international disputes. It is also important to consider how cyber warfare, as a component of a continuous and hybrid warfare strategy, impacts traditional principles of sovereignty and nonintervention.

Traditional understanding of the Westphalian system holds that violations of a nation's sovereignty, such as invasion or interference in domestic affairs, can be grounds for legitimate retaliation, often taking the form of military action (Demchak & Dombrowksi, 2011). However, in the realm of cyber warfare, this doctrine seems to be less applicable (Schmitt, 2013).

Throughout the years 2020–2022, numerous instances of cyberattacks were documented, many of which can be interpreted as violations of...
sovereignty under Westphalian principles. For example, attacks targeting critical infrastructure or government agencies directly undermine state authority and control within a nation's borders, breaching the principle of sovereignty. Similarly, spearphishing attempts and malware attacks infringe upon the principle of non-intervention, as they represent attempts to interfere in the internal affairs of a state.

Digital transformation has elevated risk to a new level with a new layer, which is the cyber layer. Risks range from impacts on critical infrastructure to increased dependence on that infrastructure due to widespread use of technologies, as well as systemic and structural risks (Stefani & Costa, 2021).

Despite these repeated violations of Westphalian principles, the response from the nations involved did not escalate to military retaliation. Even as cyber aggression remained steady and sovereignty was routinely infringed upon, it did not provoke a corresponding escalation in physical conflict until the events of February 2022.

This suggests that, at least in the context of cyber warfare, breaches of Westphalian principles do not necessarily lead to traditional military retaliation. It appears that nations may be more tolerant of violations in the digital realm, or perhaps they simply lack the established frameworks to respond in a manner equivalent to the response to physical transgressions (Schmitt, 2017).

Therefore, while cyber warfare undeniably presents challenges to the Westphalian system, it also appears to be reshaping the implications of these principles (Broeders, 2016). Violations of sovereignty and non-intervention in the cyber domain do not seem to carry the same consequences as they do in traditional warfare, reflecting a possible divergence in the norms governing cyber and physical conflicts (Broeders, 2016).
5. Conclusion

In the introduction to the study, a connection was made between the foundational Treaty of Westphalia and the situation in Ukraine, which was used as an example. The study proposed that the ideas of national sovereignty and non-intervention, central to the Treaty of Westphalia, are being tested in today’s digital age, especially during geopolitical tensions like the one between Ukraine and Russia.

A review of existing literature delved deep into the ideas behind the Westphalian system. The study explored how the concept of sovereignty and non-intervention is being redefined in an era where boundaries are not always physical. Notably, the use of digital means to influence conflicts, adding complexity to international relations, was also highlighted.

For the research, a detailed examination of a comprehensive database was done to understand the incidents between Russia and Ukraine from January 2020 to January 2022. This database helped in analyzing these incidents, their implications, and their relationship to the ongoing geopolitical tension.

The research showed that both Russia and Ukraine faced a significant number of digital incidents. However, it's crucial to understand that due to the hidden nature of these incidents, it's hard to be entirely sure of their origins. Interestingly, during the time studied, there wasn’t any evidence to suggest that Ukraine was the source of any incidents against Russia. Also, the data did not show an increase in incidents before the events in Ukraine in February 2022.

Therefore, the study did not support the idea that cyber incidents heavily influenced the principles of the Treaty of Westphalia in this context. As these incidents did not result in a direct military response, it appears that the present comprehension of these principles is capable of handling the challenges of the digital era.
References


Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a


