ULUSLARARASI İLİŞKİLER | INTERNATIONAL RELATIONS

Online First Article, 04 August 2025: 1-18
https://doi.org/10.33458/uidergisi.1747943

# Navigating the Foreign Policy in Cyber Landscape: A Novel Model for State Decision-Making in Cyberspace

Pao-wen LI
Associate Professor, Institute of China and Asia-Pacific Studies, National Sun Yat-Sen University, Kaohsiung
E-Mail: paowenl@mail.nsysu.edu.tw
Orcid: 0009-0004-7045-4689

Enescan LORCI
Research Assistant & PhD Candidate, Institute of China and Asia-Pacific Studies, National Sun Yat-Sen University, Kaohsiung
E-Mail: enescanlorci@g-mail.nsysu.edu.tw
Orcid: 0000-0003-0111-6331

**Abstract**

This study examines the interplay between cyberspace and traditional foreign policy, addressing two key questions: (1) How does cyberspace influence foreign policy decision-making? and (2) What framework can integrate factors from real and cyber politics to guide leaders during conflicts? Using a rationalist lens, this study proposes a model centered on leadership, emphasizing two variables: perceived hostility and balance of power dynamics. The model categorizes state-led cyber actions into three levels—cyber espionage, destabilization, and conflict—based on attribution risks and geopolitical conditions. Empirical analyses of cases such as Stuxnet, Russia-Ukraine, and U.S.-China cyber activities demonstrate how leaders rationally select cyber actions to navigate complex geopolitical and cyber landscapes. This research advances our understanding of cyber-enabled statecraft and offers a structured framework for policymakers to address emerging challenges in the digital age.

**Keywords:** Rational Choice, Leader, Cyber Espionage, Cyber Destabilization, Cyber Conflict

**Research Article** | Received: 16 May 2024, Last Revision: 21 July 2025, Accepted: 22 July 2025

## Introduction

International Relations (IR) theories provide diverse perspectives on foreign policy (Hudson and Vore 1995; Wohlforth 2015) but often overlook the intersection of cyberspace and traditional statecraft. As cyberspace becomes integral to national security (Choucri and Clark 2019), the lack of a unified framework linking cyberspace and foreign policy remains a critical gap. This study seeks to bridge this gap by emphasizing that political processes in cyberspace are fundamentally driven by human leadership (Choucri 2012: 23). Despite the unique characteristics of cyberspace, a consistent element is that the leaders play a pivotal role in shaping state security, sovereignty, economic stability, and international collaboration across both virtual and physical domains (Lewis 2015; Brantly 2021; Hofmann and Pawlak 2023).

Thus, this study moves beyond the technical aspects of cyberspace to focus on how national leaders perceive and navigate this evolving domain through a strategic lens. This study addresses two key questions: (1) How does cyberspace influence traditional foreign policy decision-making? (2) What framework can synthesize factors from both real and cyber politics for leaders to make decisions in times of conflict? Through theoretical inquiry and case studies, this paper will evaluate the adaptability and effectiveness of our rational model that classifies state cyber actions—espionage, destabilization, and conflict—based on leaders' perceptions of hostility and power balance and supported by empirical case studies, including Stuxnet, Russian cyber operations in Ukraine, and US-China cyber espionage. By focusing on leadership as the key decision-making agent, our model demonstrates that states are more likely to engage in specific types of cyber actions with conditions—espionage when risks are high or hostility is low, conflict when power is asymmetric and hostility is high, and destabilization when power is balanced under hostile conditions.

## The Increasing Significance of Cyberspace in IR

In IR, "space" traditionally encompasses domains that enable power projection, territorial control, and economic advantage. Choucri's (2012) concept of "cyberpolitics" redefines cyberspace as a domain of political contestation where strategic leadership, rather than technical expertise alone, determines the exercise of power. Beyond traditional domains like land, sea, air, and outer space, cyberspace has emerged as a critical arena for statecraft, presenting both opportunities and threats for foreign policy and national security decision-making. Defined as the global electromagnetic domain accessed through electronic technology (Lorents, Ottis, and Rikk 2009; Ottis and Lorents 2011), cyberspace's transnational nature demands new policy considerations for state leaders.

Firstly, the advent of cyberspace has reshaped traditional security paradigms, requiring comprehensive measures to safeguard interconnected resources from diverse threats (Andres 2012: 3; Gilad, Pecht, and Tishler 2020; Patel and Chudasama 2021). Secondly, national competitiveness in foreign policy has been redefined through advanced cybersecurity measures, robust digital infrastructure, and innovation in the digital economy (Douzet and Stéphane 2021). Thirdly, global cyber norms and standards have become a crucial arena for states to advance their interests and counter adversaries (Mueller 2020). States increasingly leverage cyberspace to achieve foreign policy goals, engage international audiences, shape national image, and facilitate public diplomacy. While cyberspace offers new opportunities and threats, its impact on conflict decision-making requires deeper examination.

Cyber warfare, or the weaponization of cyberspace, remains a tool for advancing policy goals and national interests (Libicki 2007: 256- 271; Maness and Valeriano 2016; Harold, Libicki, and Cevallos 2016). The key challenge lies in assessing its nature and effectiveness as a form of statecraft without overstating its impact (Cavelty 2008). Traditionally, state actions like mobilization and military threats have served as signaling tools in international politics (Schelling 1966: 94; Jervis 1989; Fearon 1997: 23). However, while cyber capabilities offer versatile means to influence geopolitics and gain strategic advantage, they lack the accuracy

and credibility needed for effective signaling (Harknett and Stever 2011; Rid 2013; Buchanan 2020: 5-18). Despite their growing use as a new form of statecraft, policymakers still face challenges in developing a clear cost-benefit framework to integrate cyber actions into foreign policy, unlike traditional military actions with tangible outcomes. To address this gap, this study proposes a state-level decision-making model for cyber actions. The model, in this study, focuses on the rationale behind a state's decision to initiate cyber operations against another state, categorized into three distinct levels: cyber espionage, cyber destabilization, and cyber conflict.

## A Rationalist Framework to Synthesize between Cyber and Real Politics

Cyberspace poses significant challenges for traditional foreign policymaking, yet effective leadership remains essential to bridge the gap between kinetic and digital domains through strategic vision and adaptability (Brantly 2016: 31-42). Unlike conventional military operations with discernible outcomes, cyber operations often have uncertain effects and unintended consequences (Lonergan 2017). Attribution is another major obstacle, as identifying the source of cyber-attacks is inherently complex (Brantly 2021). Additionally, the rapid pace of technological change requires leaders to continually adapt strategies to address emerging threats (Hofmann and Pawlak 2023). The interconnected nature of cyberspace further complicates responses, as cyber actions frequently cross borders, escalating diplomatic and legal costs (Lewis 2015). Despite these challenges, state leaders must safeguard national interests and achieve policy objectives by employing both advanced cyber tools and traditional diplomatic measures.

Neoclassical realists argue that while systemic factors like international power dynamics shape foreign policy, leaders' beliefs, perceptions, and actions mediate these pressures into concrete decisions (Rose 1998; Nye 1988; Slantchev 2005; Mencütek, Aras, and Coşkun 2020: 97). Building on this view, this study conceptualizes leaders as key actors bridging kinetic spaces and cyberspace, helping to address the disparities between these domains. In both kinetic and digital domains, leaders play a central role in navigating external threats and opportunities based on their perceptions and assessments. This perspective underpins our model, which positions the leader as a rational actor making strategic decisions in cyberspace.

Building on neoclassical realism, our model posits that leaders' interpretation of risks and opportunities at the international-domestic and physical-virtual nexus underpins foreign policy making in the digital age. Leaders assess international threats and opportunities through the lens of domestic politics (Beqa 2017; Rose 1998). On the one hand, leaders' perceptions play a crucial role in assessing domestic and international forces (Fearon 1995: 38).[1] On the other hand, these assessments can vary across leaders and over time.[2] Additionally, Panwar (2017)

1 However, structural realists maintain that the constraints imposed by the international system often outweigh domestic considerations, particularly in crises and conflicts (Mearsheimer and Rosato 2023; Schweller 2003).

2 For instance, Taiwan's policies toward China have shifted between administrations due to differing interpretations and assessments of China (Niou 2016).

highlights that leaders' cognitive engagement with cyberspace provides a strategic alternative without the costs of physical warfare in traditional domains like land, sea, air, and space. In short, leaders serve as pivotal actors, analyzing risks at both international and domestic levels while bridging the virtual and physical realms in the conduct of cyber operations.

A central question in IR is why conflicts, including costly wars, occur. This study adopts a rationalist approach, arguing that conflicts arise when leaders perceive the benefits as outweighing the costs (Fearon 1997: 77). In cyberspace, the focus shifts to factors shaping leaders' utility calculations and threat perceptions. Both complexity theory and constructivism highlight leadership's role in managing unpredictability and societal contexts, while rationalist theories emphasize cost-benefit calculations shaped by leaders' interpretations of domestic and international realities.[3] Leadership remains pivotal in understanding and managing conflicts in the cyber domain.

This study argues that leaders' utility calculations and threat perceptions in cyberspace are shaped by two variables: perceived hostility and the balance of power between states. Higher hostility or an unfavorable power balance increases the likelihood of cyber actions, which leaders use to advance broader diplomatic and national goals. This framework underscores how leaders integrate cyber operations into risk assessments, balancing national interests with the risks of escalation.

## The Synthesized Model

This study focuses on the "initiator state," proposing a model for utility calculations in selecting among three levels of cyber actions: espionage, destabilization, and conflict. The choice hinges on two key variables: perceived hostility and the power balance between the initiator and target. These factors are critical in assessing the risks of specific cyber actions, reflecting a rational decision-making approach. This section outlines the research design in detail.

### *Independent Variables*

Our analysis conceptualizes the perception of hostility variable along two dimensions: obvious hostility and absence of obvious hostility in bilateral relations. Obvious hostility is characterized by explicit tensions, unresolved disputes, and frequent confrontations, often rooted in territorial claims, historical grievances, or ideological divides. Absence of obvious hostility, in contrast, refers to relations where overt conflict is absent and disagreements are managed diplomatically, promoting relative stability (Lee 2018; Muncaster and Zinnes 1990; Zinnes 1962).

3 Complexity theory emphasizes the unpredictability of conflicts and the crucial role of leaders in adapting to evolving circumstances (Jervis 1989: 65; Simpson 2012; Snyder and Hui 2023). However, it is criticized for offering minimal actionable guidance for policymakers. Constructivism links conflicts to socially constructed identities, norms, and perceptions (Wendt 1999), , with leaders' actions shaped by historical relationships and collective ideas (Finnemore and Hollis 2016). Critics contend that constructivism overemphasizes ideas, overlooks power dynamics, and struggles to predict conflicts due to the fluid nature of identities and norms.

The second variable is the initiator's perceived bilateral balance of power, assessed through three conditions: initiator-favored, balanced, and target-favored. The balance of power has long been a guiding principle in state actions, particularly in conflict dynamics (Haas 1953; Nexon 2009; Müller and Albert 2021). In bilateral relations, greater power superiority reduces the initiator's perceived costs and risks of engaging in conflict.

## Dependent Variable

Since the distinction between offense and defense in cyberspace is often ambiguous (Buchanan 2020: 257), this study categorizes state-led cyber actions into three levels: cyber espionage (first level), cyber destabilization (second level), and cyber conflict (third level). These levels are defined based on the risk of attribution—the ability to trace and identify the origin or nature of a cyberattack—commonly referred to as "plausible deniability."

Cyber espionage, focused on covert information gathering, carries high plausible deniability due to its stealthy nature and minimal evidence. In contrast, cyber destabilization and cyber conflict involve overt disruption, increasing the risk of attribution and its associated costs. Plausible deniability is moderate in cyber destabilization and lowest in cyber conflict compared to cyber espionage. As attribution risk rises, so do the real-world costs for the initiator in traditional kinetic domains. Therefore, from a decision-maker's perspective, the cost and consequences in the physical realm, rather than whether an action is classified as offensive or defensive, are central to utility calculations. This framework underscores the importance of plausible deniability and attribution risk in shaping cyber strategy and decision-making.

## Hypotheses

Our model develops four hypotheses based on the interactions between two independent variables.

*H1: In the absence of perceived obvious hostility, initiator states are more likely to engage in cyber espionage.*

Cyber espionage involves covert operations to access sensitive information from governments, corporations, or high-value targets, often using Advanced Persistent Threats (APTs), phishing, zero-day exploits, man-in-the-middle (MITM) attacks, remote access trojans (RATs) and other tactics for prolonged intelligence gathering (Lindsay 2013). Attackers also use supply chain breaches, insider threats, and tools like backdoors, and keyloggers, for persistent access and control.

In the absence of overt hostility, regardless of the balance of power, cyber espionage is the most rational choice in our model, as decision-makers aim to avoid conflict escalation and maintain the status quo. Here, threat perception alone drives strategic calculations, highlighting the importance of leadership in shaping cyber actions. In international politics, shifting alliances mean today's allies may become tomorrow's adversaries. Rational decision-makers engage in espionage during peacetime to prepare for potential future hostilities. For

instance, the United States (US) has conducted cyber espionage against allies like Germany and Japan during periods of relative peace. These cases will be discussed in the following section.

*H2: When a perception of obvious hostility is combined with an initiator-favored bilateral balance of power, initiator states are more likely to engage in comprehensive cyber conflict.*

The perception of obvious hostility intensifies the need for prompt decision-making, leading leaders to assess threats and power dynamics to determine the most rational course of action. In scenarios of clear hostility and a power imbalance favoring the initiator, utility calculations may favor comprehensive cyber conflict. This involves cyberattacks targeting government or civilian infrastructure, causing significant disruption and advancing strategic or military objectives (Robinson, Jones, and Janicke 2015; Lindsay 2013).

Our model suggests that comprehensive cyber conflict often precedes conventional military conflict, as states use cyberattacks to weaken adversaries' infrastructure or military capabilities (Zilincik and Duyvesteyn 2023). In such cases, where military conflict appears imminent, the risks of attribution may become secondary. When the balance of power favors the initiator, a rational leader may prioritize accelerating military objectives through cyber conflict. For example, Russia's cyberattacks against Ukraine ahead of its military invasion illustrate this strategy and will be analyzed in the next section.

*H3: When a perception of obvious hostility is combined with a target-favored bilateral balance of power, initiator states are more likely to resort to cyber espionage.*

In situations of clear hostility where the balance of power favors the target state, cyber espionage emerges as a rational strategy. Techniques such as APTs, phishing, zero-day exploits, MITM attacks, and RATs offer low-risk alternatives to overt military actions. In these circumstances, while hostility necessitates a response, the unfavorable power balance makes military escalation irrational. Cyber espionage provides plausible deniability, minimizes escalation risks, and aligns with strategic objectives to narrow the power gap. For instance, China's cyber espionage against the US to reduce the military power gap illustrates this approach and will be analyzed further in this study.

*H4: When a perception of obvious hostility is combined with balanced bilateral power dynamics, initiator states are more likely to engage in cyber destabilization.*

Cyber destabilization operations aim to disrupt a target's political, economic, or social stability. Methods include Distributed Denial of Service (DDoS) attacks, targeting critical infrastructure like power grids or transportation systems, as seen in the 2015 Ukraine power grid attack. Disinformation campaigns and cyber propaganda, such as Russian interference in the 2016 US presidential election, manipulate public opinion and erode institutional trust. Election interference and ransomware attacks, like WannaCry in 2017, undermine democratic processes and cripple vital services. Wiper malware, exemplified by the NotPetya attack, destroys data to cause widespread damage (Lorci 2024).

Financial destabilization through attacks on banks or stock exchanges, supply chain attacks compromising third-party vendors, and data breaches like the 2016 DNC hack further illustrate these tactics. Defacement of high-profile websites and publicizing stolen information also provoke outrage and instability, making cyber destabilization a versatile tool for undermining adversaries (Buchanan 2020: 167).

A notable example of cyber destabilization is Stuxnet, a cyberattack attributed to the US and Israel targeting Iran's nuclear program. By disrupting the software controlling Iran's nuclear centrifuges, Stuxnet inflicted physical damage without a military strike, demonstrating the potential of cyber operations to sabotage critical infrastructure (Lindsay 2013: 378)

In situations of perceived hostility with a balanced power dynamic, cyber destabilization may be the most rational choice for the initiator. This approach involves malicious activities aimed at disrupting critical infrastructure, financial systems, or societal functions within the target state (Buchanan 2020:180). Unlike comprehensive cyber conflict, cyber destabilization does not serve as a prelude to military conflict but rather reflects the initiator's uncertainty about escalating to war.

In such scenarios, evident hostility compels decision-makers to respond, but the absence of a power advantage makes comprehensive cyber conflict impractical. Instead, cyber destabilization emerges as a rational choice, as it addresses pressure to act while weakening the adversary's position in the bilateral power dynamic. Although moderate attribution risks exist, the balanced power dynamic reduces the target state's likelihood of escalating to full-scale conflict. Moreover, destabilization can shift the balance of power in the initiator's favor, even if retaliation occurs.

All hypotheses are summarized in Table 1.

**Table 1.** The Synthesized Model

| Perceived Hostility \ Balance of Power | Initiator-Favored | Balanced | Target-Favored |
|---|---|---|---|
| **Obvious Hostility** | H2: Cyber Conflict | H4: Cyber Destabilization | H3: Cyber Espionage |
| **Absence of Obvious Hostility** | H1: Cyber Espionage | H1: Cyber Espionage | H1: Cyber Espionage |

## Case Study and Empirical Analysis

This section examines cases corresponding to specific hypotheses derived from the framework, based on the independent variables of perceived hostility and balance of power. While attribution challenges—such as the covert nature of operations and deniable tactics—often obscure the full scope of cyber activities, this study selects cases of significance in cyber and international

relations. These cases are supported by extensive documentation and empirical richness, enabling reliable process tracing and enhancing the model's explanatory power. Despite data limitations, the selected cases systematically represent variations in power dynamics, hostility levels, and the spectrum of cyber actions, from espionage to conflict, offering a comparative understanding of cyber decision-making.

## *Cyber Espionage (H1)*

This section examines the first hypothesis: In the absence of perceived obvious hostility, initiator states are more likely to engage in cyber espionage.

The first case is the US's cyber espionage campaigns against Germany. In 2013, reports emerged alleging that the US had been conducting widespread surveillance on its allies, including Germany. It was revealed when former US National Security Agency (NSA) contractor Edward Snowden leaked classified documents to the media, that the NSA had been monitoring German Chancellor Angela Merkel's communications. Espionage activities undertaken by the US under the pretext of national security interests were primarily aimed at gaining political and diplomatic insights and enhancing alliance management.

The second case is the United Kingdom's cyber espionage campaigns against European Union (EU) members. The UK has been accused of conducting cyber espionage against various EU member states, including France, Germany, and Belgium. These espionage activities, allegedly carried out by intelligence agencies such as the Government Communications Headquarters (GCHQ), have targeted government officials, diplomats, and European institutions (The Guardian 2018).

Finally, the third case is Israel's reported cyber espionage activities against the US. In the past, there have been allegations and reports suggesting that Israeli intelligence agencies, such as the Mossad, have conducted cyber operations, including espionage, targeting the US (Stein 2016). These activities have often been linked to Israel's security interests and its efforts to gather intelligence on matters of strategic importance. However, specific details regarding such incidents are typically closely guarded, and official confirmations or denials are rare.

These three cases provide strong support for our first hypothesis for several reasons. First, the countries involved in these cyber espionage cases do not demonstrate a perception of obvious hostility but instead share aligned views on key international issues. For example, both the US and Germany perceive Russia as a significant threat, particularly regarding NATO's collective defense. Both nations regard NATO as essential to transatlantic security and remain committed to countering Russian aggression.

Additionally, the UK and EU member states have also collaborated extensively to combat radicalization and violent extremism, both online and offline. Joint initiatives have focused on enhancing societal resilience against extremist ideologies and dismantling terrorism-supporting networks. For instance, their cooperation in intelligence sharing and counter-terrorism operations has been facilitated through platforms such as Europol and the European Counter Terrorism Centre. These efforts have enabled the exchange of critical

intelligence, coordinated operations, and strengthened collective capabilities to prevent and respond to terrorist threats effectively.

Finally, Israel and the US collaborate closely on critical security issues, including efforts to counter the proliferation of weapons of mass destruction (WMDs), particularly nuclear weapons, in the Middle East. Their joint efforts to monitor and curb Iran's nuclear ambitions involve extensive intelligence sharing, coordinated diplomatic initiatives, and alleged covert operations, such as the Stuxnet cyberattack, which disrupted Iran's nuclear facilities to delay its progress toward developing nuclear weapons.

The second factor supporting the suitability of these cases for our model pertains to the balance of power variable. Empirical evidence demonstrates that in the absence of perceived obvious hostility, states engage in cyber espionage regardless of power dynamics. For instance, in the first case, despite a power advantage, the US conducted cyber espionage against Germany. In the second case, with relatively balanced power, the UK engaged in cyber espionage against EU member states. Lastly, in the third case, despite the U.S. holding a power advantage, Israel still initiated cyber espionage against it. These cases illustrate that when hostility is not perceived, decision-makers rationally resort to cyber espionage irrespective of the bilateral balance of power.

In short, the three cases examined provide substantial support the first hypothesis, demonstrating that in the absence of perceived obvious hostility, states rationally engage in cyber espionage irrespective of the bilateral balance of power. This analysis underscores the utility of cyber espionage as a low-risk, rational choice for states operating within cooperative yet competitive international environments.

## *Cyber Conflict (H2)*

This section examines the second hypothesis: When a perception of obvious hostility is combined with an initiator-favored bilateral balance of power, initiator states are more likely to engage in comprehensive cyber conflict.

The Russian invasion of Ukraine highlighted the integration of cyber warfare with traditional military tactics. Before the invasion, Russia conducted widespread cyberattacks, targeting the Ukrainian government and non-governmental sectors, including state agencies, banks, and critical infrastructure. Key incidents included the defacing government websites in January, 2022, DDoS attacks on banking and defense systems in February, 2022, and destructive cyber operations against media outlets, government agencies, and nuclear facilities during the invasion. These coordinated attacks aimed to disrupt Ukraine's infrastructure and intimidate its population, demonstrating the evolving role of cyber operations in modern conflict (Kolodii 2024).

For several reasons, the Russian cyber warfare campaign against Ukraine serves as a compelling case study for third-level cyber action (cyber conflict) within our analytical framework. Firstly, this case meets the criteria for "perception of obvious hostility," reflecting the prolonged enmity between Russia and Ukraine. Key triggers include Ukraine's geopolitical

pivot toward NATO and the EU, exemplified by the 2014 Euromaidan protests that ousted pro-Russian president Viktor Yanukovych. These developments were perceived by Russia as direct threats to its regional influence and strategic interests, given Ukraine's historical and cultural ties to Russia (Kösen and Gezer 2025). The annexation of Crimea further escalated hostilities, fueling armed conflict in Eastern Ukraine between Ukrainian forces and pro-Russian separatists, supported militarily and politically by Russia (Kösen and Gezer 2025). By 2022, this prolonged conflict and Russia's heightened sense of insecurity culminated in decisive actions, reflecting the interplay of strategic imperatives and perceived threats (Lewis 2022).

Secondly, as Russia's sense of insecurity grew, its strategic focus increasingly centered on the initiator's perception of balance of power dynamics concerning Ukraine. Russian decision-makers initially anticipated a swift resolution, expecting Ukraine to capitulate within weeks (Kolodii 2024). This expectation reflects a belief among Russian strategists that they held a favorable position as the conflict's initiator within the broader geopolitical context. However, the authoritarian nature of the Russian regime likely distorted the quality of information informing these assessments, shaping perceptions of the bilateral balance of power. Ultimately, the leader's final decision was influenced by a regime-driven, potentially biased interpretation of these dynamics.

Thirdly, Russia's use of cyber warfare during its invasion of Ukraine aligns closely with our conceptualization of cyber conflict, as these operations were strategically designed to advance military objectives. Russian cyber campaigns targeted critical governmental, military, and economic infrastructure, aiming to degrade, disrupt, or dismantle key systems, control critical networks, and impede information access for the Ukrainian populace. Microsoft Corporation's analysis corroborates this alignment, highlighting the coordination between Russia's cyber operations and kinetic military actions. For example, during a missile strike on Kyiv's TV tower on March 1, 2022, media organizations in the capital suffered simultaneous destructive cyberattacks (Kolodii 2024). Similarly, cyber intrusions targeting critical infrastructure in Sumy preceded widespread electricity shortages, demonstrating the strategic synchronization of cyber and military offensives. These coordinated actions reflect deliberate decision-making and the integration of cyber warfare into Russia's broader military strategy against Ukraine (Thornton and Miron 2022).

Building on the strategic coordination of cyber operations and military actions during the Russian invasion of Ukraine, another critical aspect of Russia's cyber warfare campaign is its ability to adapt tactics in response to shifting battlefield dynamics. As initial assessments of a swift victory proved inaccurate, Russian decision-makers recalibrated their cyber strategies, transitioning from high-intensity operations to more targeted approaches. In the early phase of the conflict, destructive cyber incidents surged, with malware such as FoxBlade, IsaacWiper, DesertBlade, and SecureDelete deployed, resulting in 22 significant events during the first week of hostilities. However, the frequency of such operations declined in subsequent weeks, with only 15 incidents recorded over the following five weeks (Kolodii 2024). As Russian forces redeployed from Kyiv to Eastern and Southern Ukraine, preparing for a protracted

conflict, cyber tactics evolved further. This shift underscores the critical role of decision-makers in recalibrating cyber strategies to align with changing operational priorities and battlefield dynamics.

In short, the Russian cyber warfare campaign against Ukraine demonstrates how decision-makers strategically employ cyber operations in response to the interplay between threat perceived hostility and balance of power. By adapting cyber tactics to evolving battlefield conditions, Russia's actions highlight the rational decision-making processes underpinning the use of cyber conflict as an integral component of statecraft.

### *Cyber Espionage (H3)*

This section examines the third hypothesis: When a perception of obvious hostility is combined with a target-favored bilateral balance of power, initiator states are more likely to resort to cyber espionage.

China's cyber espionage campaign, which intensified in the early 2000s, has become increasingly sophisticated, targeting countries such as the US, UK, Taiwan, and Germany through tactics like spear-phishing. Driven by economic and geopolitical objectives, China is alleged to have stolen designs for over two dozen US weapons systems, including the F-35 fighter jet and Patriot missiles (Jones 2020).

A prominent case of China's cyber espionage strategy is Su Bin, a Chinese businessman linked to espionage in the aviation and aerospace sectors, illustrating efforts to narrow gaps in commercial and military capabilities. From 2009 to 2014, Su collaborated with two Chinese military hackers to steal over 630,000 files from Boeing, including detailed data on the C-17 cargo aircraft, as well as the F-22 and F-35 fighter jets. Acting as a facilitator, Su guided target selection, identified specific technologies, companies, and individuals, translated the stolen information into Chinese, and provided reports to the General Staff Headquarters of the People's Liberation Army of China, emphasizing the data's strategic importance. This theft significantly accelerated China's development of its own C-17 derivative, the Xi'an Y-20, unveiled in 2014, underscoring the rapid advancement of its military aviation capabilities (Jones 2020). Beyond aviation, Chinese hacking groups have targeted classified information related to the US Pacific Command, a critical entity in potential conflicts involving China. Their efforts have also focused on the logistical frameworks of US military operations, including aerial refueling missions essential for Pacific theater operations. These activities reflect China's broader strategy of using cyber espionage to narrow military capability gaps with the US.

The case of Su Bin serves as a compelling example of first-level cyber actions, cyber espionage, within the framework of our model in scenarios defined by the combination of "perceived hostility" and "target-favored bilateral balance of power". This case is particularly relevant for several reasons. First, the evident hostility between China, the initiator, and the US, the target, aligns with our conceptual framework. This hostility is reflected in geopolitical competition, ideological differences, trade tensions, and military rivalries, all contributing to a climate of strategic rivalry.

Secondly, the US holds a distinct advantage over China in terms of the balance of power. Historically, China has trailed the US in economic and military capabilities, lacking the technological sophistication and global influence that underpin American dominance (Sánchez and Akyesilmen 2021). Confronted with this power asymmetry, Chinese decision-makers adopted cyber espionage as a rational strategy to bridge the gap while mitigating risks. By targeting sensitive information and intellectual property, these campaigns aimed to reduce technological disparity and challenge US military superiority. The emphasis on plausible deniability ensured that these operations remained covert, allowing Chinese actors to persist within American networks undetected for extended periods. Consequently, China was able to develop military capabilities that rival those of the US, effectively reducing the balance gap at a fraction of the cost and time investment incurred by its adversary.

To summarize, the case of Su Bin supports the third hypothesis. It demonstrates that in scenarios of perceived hostility combined with a target-favored balance of power, initiator states rationally resort to cyber espionage. China's actions highlight how cyber espionage can enables states to bridge capability gaps and challenge adversaries at minimal cost and risk, aligning with the model's predictions.

## *Cyber Destabilization (H4)*

This section examines the fourth hypothesis: When a perception of obvious hostility is combined with balanced bilateral power dynamics, initiator states are more likely to engage in cyber destabilization.

In June 2010, analysts identified Stuxnet, a highly sophisticated computer worm attributed to US and Israeli intelligence, designed to disturb Iran's nuclear program by sabotaging its nuclear centrifuges. As part of the broader "Olympic Games" cyber campaign, Stuxnet infiltrated industrial control systems by exploiting software vulnerabilities and Siemens default passwords, causing extensive damage to Iran's Natanz facility. The attack significantly delayed Iran's nuclear progress, with a Mossad official estimating a postponement of nuclear weapon development until 2015, highlighting the effectiveness of US-Israeli collaboration (Buchanan 2020: 104).

The case of Stuxnet offers a compelling example of level two cyber action (cyber destabilization) within our framework. First, the attack occurred in the context of significant hostility between the initiators, the US and Israel, and the target, Iran, driven by historical grievances, ideological differences, and geopolitical competition in the Middle East. At the time, the US and Israel viewed Iran's nuclear program as a direct threat to their security interests, exacerbated by Iran's hostile rhetoric toward Israel and its support for regional militant groups. These security concerns formed the basis for the joint effort to undermine Iran's nuclear ambitions through cyber destabilization.

Secondly, the initiators' perception of balance of power dynamics highlights the significance of the Stuxnet case within our framework. Both Israel and the US sought to curb Iran's aspirations for regional dominance. By 2009, when Stuxnet was launched, the

US, despite its global superiority, perceived an unfavorable balance of power in addressing Iran's nuclear ambitions. Quick military strikes were deemed unfeasible due to concerns over casualties, diplomatic backlash, and a lack of domestic support. Furthermore, the 2007 US National Intelligence Estimate publicly stated that Iran had not decided to restart its nuclear weapons program, weakening the justification for military action (NIC 2007). These constraints prompted the Bush administration to explore alternatives after the failure of economic sanctions and diplomatic efforts (Mohee 2022). Recognizing that the costs of military intervention outweighed the potential benefits, the US shifted to non-traditional strategies, such as cyber operations and covert actions. These approaches offered a cost-effective and politically viable means to address security threats and advance national interests while minimizing risks.

Thirdly, the potential divergence in US-Israel cooperation toward Iran further complicated the perceived balance of power dynamics. Situated in close proximity to Iran and viewing itself as the primary target of a potential Iranian nuclear arsenal, Israel regarded Iran's nuclear program as a more immediate and existential threat than the US did. This heightened concern led Israel to intensify lobbying efforts for decisive action. In early 2008, the Israeli government secretly requested bunker-busting bombs from the Bush administration to enhance its capacity to neutralize Iran's underground nuclear facilities. These munitions were intended for precision strikes on key Iranian targets, including underground bunkers and refueling sites, while ensuring Israeli aircraft could return safely to their airspace (Mohee 2022). The Bush administration ultimately rejected Israel's request, citing concerns that utilizing Iraqi airspace for such operations could provoke significant backlash. The potential for political unrest in Iraq, which could endanger American forces stationed there, outweighed the strategic imperative of supporting Israel's military objectives against Iran (Buchanan 2020: 234). The US adopted a pragmatic approach to advancing its strategic goals. By prioritizing feasible and cost-effective alternatives, the US aimed to address the shared threat while safeguarding its interests and those of its ally, Israel (Mohee 2022).

The US thus initiated a cyber operation to destabilize Iran's nuclear program, employing a covert and deniable approach to undermine its capabilities without resorting to overt military action. By leveraging cyber tools, the US maintained plausible deniability, minimizing the political, diplomatic, and military risks associated with a conventional strike. Additionally, the operation delivered a lasting impact by delaying Iran's nuclear progress while fostering uncertainty and mistrust within its nuclear infrastructure.

The decision to employ cyber destabilization rather than a military operation against Iran's nuclear program reflected a calculated strategy to achieve objectives with minimal risk and maximum efficiency in a complex geopolitical environment. This case aligns with the analytical framework, demonstrating how decision-makers, faced with a perception of hostility and a not so favorable balance of power, rationally opted for cyber destabilization to advance strategic goals while avoiding the high costs and risks of conventional military conflict.

The results of the case study are summarized in Table 2. As shown in the table, cyber espionage emerges as the most common action in cyberspace for initiators, requiring only one

condition to be met. In scenarios lacking perceived hostility or under a target-favored balance of power, initiators are more likely to employ cyber espionage to advance their strategic interests. The cases of US-Germany, UK-EU, Israel-US, and China-US espionage provide strong support for H1 and H3.

**Table 2.** The Synthesized Model with Empirical Cases

| Perceived Hostility \ Balance of Power | Initiator-Favored | Balanced | Target-Favored |
|---|---|---|---|
| **Obvious Hostility** | Russian Cyber Conflict in Ukraine (H2) | Joint Cyber Operation of the US and Israel against Iran: Stuxnet (H4) | China's Cyber Espionage Campaigns against the US (H3) |
| **Lack of Obvious Hostility** | The US's Cyber Espionage Campaigns against Germany (H1) | The UK's Cyber Espionage Campaigns against European Union Members (H1) | Israel's Cyber Espionage Campaigns against the US (H1) |

Conversely, cyber destabilization and cyber conflict require two conditions to be met. The Russia-Ukraine case supports H2, demonstrating that comprehensive cyber conflict occurs when obvious hostility is combined with an initiator-favored balance of power. Similarly, the US-Iran Stuxnet case supports H4, indicating that cyber destabilization arises in scenarios of obvious hostility and a balanced power dynamic (Table 2).

## Conclusion

This study addresses two key questions: (1) How does cyberspace influence traditional foreign policy decision-making? and (2) What framework can synthesize factors from both real and cyber politics for leaders to make decisions in times of conflict? It contributes to the theoretical understanding of cyberspace as an extension of traditional statecraft by offering a structured framework for analyzing how states integrate cyber actions into foreign policy. The model emphasizes the central role of leadership in assessing risks, calculating utility, and adapting strategies within both kinetic and virtual domains.

To answer the first question, this study highlights the need to bridge the gap between cyber and traditional politics. Cyberspace influences foreign policy by providing states with flexible, scalable, and covert tools to navigate complex strategic environments. Decision-makers are compelled to incorporate cyber capabilities into their strategic calculus, adapting both traditional and novel approaches to account for the unique risks and opportunities of the digital domain. This integration reshapes the conduct of statecraft, positioning cyberspace as a critical arena in contemporary international relations.

For the second question, the framework centers on leadership, synthesizing cyber-specific dynamics—such as plausible deniability and covert operations—with traditional

geopolitical variables like balance of power and perceived hostility. These cyber-specific dynamics define the risks of actions in cyberspace, while the geopolitical variables form the foundation for predicting the type of cyber action a leader might initiate. Through a series of hypotheses, the study delineates scenarios in which leaders are likely to adopt cyber espionage, destabilization, or conflict based on utility calculations and risk assessments, navigating the interplay of the physical and virtual realms.

The study further emphasizes the necessity for continuous adaptation in response to evolving cyber threats and technological advancements. By situating cyber actions within broader strategic objectives and risk assessments, leaders can safeguard national interests while minimizing the potential for escalation in the real world. In essence, this study advances our understanding of the evolving dynamics of international relations in the digital age, highlighting the pivotal role of leadership in managing the complexities of cyberspace. By offering a theoretical framework supported by empirical insights, this study provides valuable tools for policymakers, scholars, and practitioners seeking to address the challenges and opportunities posed by cyberspace. It demonstrates how leaders can effectively integrate cyber capabilities into foreign policy to navigate the interconnected realities of modern geopolitics.

## References

Andres, Richard B. 2012. The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. In *Cyberspace and National Security: Threats, Opportunities, and Power in Virtual World*. ed. Derek S. Reveron. Washington DC, Georgetown University Press: 89–104.

Brantly, Aaron Franklin. 2016. *The Decision to Attack: Military and Intelligence Decision-Making*. Athens, University of Georgia Press.

Brantly, Aaron Franklin. 2021. Risk and Uncertainty Can Be Analyzed in Cyberspace. *Journal of Cybersecurity* 7, 1: 1–12.

Beqa, Mentor. 2017. Neoclassical Realism : Its Promises and Limits as a Theory of Foreign Policy. *European Academic Research* 1: 1–16.

Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Global Security and Intelligence Studies*. Cambridge, Harvard University Press.

Cavelty, Myriam Dunn. 2008. Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology and Politics* 4, 1: 19–36.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. London, The MIT Press.

Choucri, Nazli and David D. Clark. 2019. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, The MIT Press.

Douzet, Frédérick and Taillat Stéphane. 2021. Prepping for Long-Term Competition? U.S. Leadership in Cyberspace from Trump to Biden. In *US Leadership in a World of Uncertainties*, ed. Michael Stricof and Isabelle Vagnoux. London, Palgrave Macmillan

Fearon, James D. 1995. Rationalist Explanations for War. *International Organization* 49, 3: 379–414.

Fearon, James D. 1997. Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs. *Journal of Conflict Resolution* 41, 1: 68–90

Finnemore, Martha and Duncan B Hollis. 2016. Constructing Norms for Global Cybersecurity. *American Journal of International Law* 110, 3: 425–479.

Gilad, Amitai, Eyal Pecht and Asher Tishler. 2020. Intelligence, Cyberspace, and National Security. *Defence and Peace Economics* 32, 1: 18–45.

Haas, Ernst B. 1953. The Balance of Power as a Guide to Policy-Making. *The Journal of Politics* 15, 3: 370–398.

Harknett, Richard J. and James A Stever. 2011. The New Policy World of Cybersecurity. *Public Administration Review* 71, 3: 455–560.

Harold, Scott, Martin Libicki and Astrid Cevallos. 2016. *Getting to Yes with China in Cyberspace*. Rand Corporation.

Hudson, Valerie. M. and Christopher. S. Vore. 1995. Foreign Policy Analysis Yesterday, Today, and Tomorrow. *Mershon International Studies Review* 39, 2: 209–238.

Hofmann, Stephanie C. and Patryk Pawlak. 2023. Governing Cyberspace: Policy Boundary Politics across Organizations. *Review of International Political Economy* 30, 6: 2122–2149.

NIC. 2007. *Iran: Nuclear Intentions and Capabilities*. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20071203_release.pdf (accessed June 25, 2024).

Jervis, Robert. 1998. *System Effects: Complexity in Political and Social Life*. Princeton, Princeton University Press.

Jones, Jeff B. 2020. *Confronting China's Efforts to Steal Defense Information*. National Security Fellowship Program Belfer Center for Science and International Affairs Harvard Kennedy School.

Kolodii, Roman. 2024. The Pedagogy of Cyber-WAR: Explaining Ukraine's Resilience against Russian Cyber-Aggression. *Defense and Security Analysis* 40, 2: 1–22.

Kösen, Mustafa Gökcan and Ş. Gökçe Gezer. 2025. Emotion Norms and International Securitization in Foreign Policy Analysis: The Official Russian Narratives on the Ukrainian-Russian War. *Uluslararası İlişkiler* Advanced Online Publication: 1–20.

Lee, Melissa M. 2018. The International Politics of Incomplete Sovereignty: How Hostile Neighbors Weaken the State. *International Organization* 72, 2: 283–315.

Lewis, James A. 2015. *Statement before the House Committee on Foreign Affairs: Cyber War: Definitions, Deterrence, and Foreign Policy*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/ts150930_Lewis.pdf (accessed June 25, 2024).

Lewis, James A. 2022. Cyber War and Ukraine. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash (accessed July 20, 2024).

Libicki, Martin C. 2007. *Conquest in Cyberspace National Security and Information Warfare*. New York, Cambridge University Press.

Lindsay, Jon R. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22, 3: 365–404.

Lonergan, Shawn William. 2017. *Cyber Power and the International System*. PhD Thesis, Columbia University.

Lorci, Enescan. 2024. Ben Buchanan, The Hacker, and the State: Cyber Attacks and the New Normal of Geopolitics (Harvard University Press, 2020), *Uluslararası İlişkiler* Advanced Online Publication, 24 May: 1-3.

Lorents, Peeter, Rain Ottis and Raul Rikk. 2009. Cyber Society and Cooperative Cyber Defence. In *Internationalization, Design and Global Development*, ed. Nuray Aykin. Berlin, Heidelberg: Springer Berlin Heidelberg: 180-186.

Maness, Ryan C. and Brandon Valeriano. 2016. The Impact of Cyber Conflict on International Interactions. *Armed Forces and Society* 42, 2: 301–323.

Mearsheimer, John J. and Sebastian Rosato. 2023. *How States Think: The Rationality of Foreign Policy.* London, Yale University Press.

Mencütek Şahin, Zeynep N., Ela Gökalp Aras and Bezen Balamir Coşkun. 2020. Turkey's Response to Syrian Mass Migration: A Neoclassical Realist Analysis. *Uluslararası İlişkiler* 17, 68: 93–111.

Mohee, Ahmad. 2022. A Realistic Analysis of the Stuxnet Cyber-Attack. *MA Arabic Studies – Political Sciences*, 1–11.

Mueller, Milton L. 2020. Against Sovereignty in Cyberspace. *International Studies Review* 22, 4: 779–801

Müller, Thomas, and Mathias Albert. 2021. Whose Balance? A Constructivist Approach to Balance of Power Politics. *European Journal of International Security* 6, 1: 109–128.

Muncaster, Robert G. and Dina A. Zinnes. 1990. Structure and Hostility in International Systems. *Journal of Theoretical Politics* 2, 1: 31–58.

Nexon, Daniel H. 2009. The Balance of Power in the Balance. *World Politics* 61, 2: 330–359.

Niou, Emerson. 2016. The China Factor in Taiwan's Domestic Politics. In *Democratization in Taiwan*, ed. Philip Paolino and James Meernik. London, Routledge: 185–200.

Nye, Joseph S. 1998. Neorealism and Neoliberalism. *World Politics* 40, 2: 235-251.

Ottis, Rain, and Peeter Lorents. 2011. Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, US, 8-9 April: 267-270.

Panwar, R. S. 2017. 21st Century Warfare: From "Battlefield" to "Battlespace". https://futurewars.rspanwar.net/21st-century-warfare-from-battlefield-to-battlespace/. (accessed July, 20, 2024).

Patel, Kathan and Dhaval Chudasama. 2021. National Security Threats in Cyberspace. *National Journal of Cyber Security Law* 4, 1: 2–10

Rid, Thomas. 2013. Cyberwar and Peace: Hacking Can Reduce Real-World Violence. *Foreign Affairs* 92, 6: 77–87.

Robinson, Michael., Kevin Jones and Helge Janicke. 2015. Cyber Warfare: Issues and Challenges. *Computers & Security* 49: 70–94.

Rose, Gideon. 1998. Neoclassical Realism and Theories of Foreign Policy. *World Politics* 51, 1: 144–172.

Sánchez, Karina, and Nezir Akyesilmen. 2021. Competition for High Politics in Cyberspace: Technological Conflicts Between China and the USA. *Polish Political Science Yearbook* 50, 1: 43-69.

Schelling, Thomas C. 1966. *Arm And Influence*. Yale University Press.

Schweller, Randall L. 2003. The Progressiveness of Neoclassical Realism. In *Progress in International Relations Theory: Appraising the Field*, ed. Colin Elman and Miriam Fendius Elman. London, The MIT Press: 68-99.

Slantchev, Branislav L. 2005. *State and Anarchy*. https://www.yumpu.com/en/document/view/12153178/introduction-to-international-relations-lecture-2-state-and-anarchy (accessed November 1, 2024).

Simpson, Emile. 2012. *War From the Ground up: Twenty-First Century Combat as Politics*. Oxford University Press.

Snyder, Greta Fowler and Andre Hui. 2023. Complexity and Quantum in International Relations. *Oxford Research Encyclopedia of International Studies*, 1–26.

Stein, Jeff. 2016. *Israel Flagged as Top Spy Threat to U.S. in New Snowden/NSA Document.* https://www.newsweek.com/israel-flagged-top-spy-threat-us-new-snowdennsa-document-262991 (accessed February 26, 2016).

*The Guardian.* 2018. British Spies 'Hacked into Belgian Telecoms Firm on Ministers' Orders.' September.

Thornton, Rod, and Marina Miron. 2022. Winning Future Wars: Russian Offensive Cyber and Its Vital Importance. *The Cyber Defense Review* 7, 3: 117–135.

Wendt, Alexander. 1999. *Social Theory of International Politics*. Cambridge, Cambridge University Press.

Wohlforth, William C. 2016. Realism and Foreign Policy. In *Foreign Policy Theories, Actors, Cases*. ed. Steve Smith, Amelia Hadfield, and Tim Dunne. Oxford University Press: 381–396.

Zilincik, Samuel and Isabelle Duyvesteyn. 2023. Strategic Studies and Cyber Warfare. *Journal of Strategic Studies* 46, 4: 836–857.

Zinnes, Dina A. 1962. Hostility in International Decision-Making. *Journal of Conflict Resolution* 6, 3: 236–243.