An Unexpected Link between Export Sanctions and Cyberespionage*

In Tae YOO** and Juwon LEE***

Abstract

Do export controls cause cyberespionage? Despite significant interest in both export controls and cyberespionage, the link between them remains understudied. This article argues that when export controls restrict a target country's access to advanced technology, it may resort to cyberespionage as a workaround. A 2SRI analysis of 747,716 directed dyad–year cases from 2001 to 2020 shows that countries under export sanctions are more likely to conduct cyberespionage attacks against sanctioning countries during this period. Case studies of North Korea and China further illustrate how export controls can drive cyberespionage. These empirical findings support our hypothesis, suggesting that states may conduct cyberespionage as a means of circumventing export controls.

Keywords: Export Controls, Cyberespionage, Economic Sanctions, Cyberattacks, Cybersecurity, Technology Security

Received Jun 10, 2025 | Reviewed Jun 23, 2025 | Accepted Aug 5, 2025 | Published Apr 30, 2026

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020S1A3A2A01095177).

** First and corresponding author. In Tae YOO (iqewoup@gmail.com; ORCID: https://orcid.org/0000-0002-8711-5112) is an Associate Professor in the Department of Political Science and International Relations at Dankook University. He received his Ph.D. in Political Science from the University of South Carolina. His research interests include cybersecurity, economic and supply chain security, emerging technologies, and internet governance, examined through the lenses of international security and international political economy. His work focuses on the intersections of these areas and their political implications for strategic rivalry

*** Part of this article includes a revised and developed version of a paper that received the Excellence Prize in the 'Cyber Security Paper Competition 2024' hosted by the National Intelligence Service and organized by the Korea Association of Cybersecurity Studies.

Juwon LEE (juwon918@gmail.com; ORCID: https://orcid.org/0009-0004-2552-8036) is an undergraduate student majoring in Political Science and International Relations at Dankook University. His research interests include Economic Security and Cybersecurity.

The Korean Journal of International Studies Vol.24, No.1 (April 2026), 65-91
https://doi.org/10.14731/kjis.2026.04.24.1.65

INTRODUCTION

Cyberespionage has prompted growing concern around the world. Most notably, though not exclusively, the United States, amid its strategic competition with China, has elevated cyberespionage to a central issue in international politics. Richard Clarke, special advisor on cybersecurity in the George W. Bush administration, warned that the United States would lose the competition "as company after company in the United States spends millions, hundreds of millions, in some cases billions of dollars on R&D and that information goes free to China," and thus, the "greatest fear is that rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts" (Rosenbaum 2012). Similarly, the chairman of the US House Intelligence Committee alleged, "There is a concerted effort by the government of China to get into the business of stealing economic secrets to put into use of in China to compete against the U.S. economy" (Schlesinger 2012). In 2012, General Keith Alexander, then director of the U.S. National Security Agency and commander of Cyber Command, called cyberespionage "the greatest transfer of wealth in history" (Rogin 2012). In July 2024, the U.S. Cybersecurity and Infrastructure Security Agency released a cybersecurity advisory on North Korean cyberespionage. According to the advisory, Andariel, a state-sponsored cyber organization under the third bureau of North Korea's Reconnaissance General Bureau (RGB), is conducting cyberespionage targeting the technical information and intellectual property of defense, aerospace, nuclear, and engineering-related organizations, while financing its operations through ransomware (Cybersecurity and Infrastructure Security Agency 2024).

China has allegedly sought to close the technology gap by stealing advanced technologies from Western industrialized nations. In response, the United States has adopted export controls to maintain a technological edge over China. Cyberespionage is not limited to China and North Korea; other states, notably Russia and Iran, also engage in such activities. Importantly, for countries restricted from legitimate transactions by economic sanctions—particularly export controls on dual-use goods—cyberespionage has become a new avenue to acquire not only enormous financial resources but also advanced technology. Cyberattacks have been on the rise, particularly in the form of cyberespionage aimed at stealing technological information, as competition in the security and economic domains among strategic rivals has intensified (Blackwell and Harris 2016; Buchanan 2020; Segal 2016). Accordingly, we observe a simultaneous increase in both export control measures and cyberespionage.

Existing studies, however, seldom analytically examine the conditions under

which states commit economic and industrial espionage, let alone cyberespionage. Only a few studies exist (Akoto 2024). To address this gap, this study asks whether export sanctions lead to cyberespionage, thereby identifying a key condition under which states are incentivized to engage in such activities. Whereas most studies address either espionage or economic sanctions separately, this research highlights the seemingly paradoxical and previously unexamined relationship between the two phenomena. It is paradoxical that export controls, designed to prevent adversaries from advancing technologically, may instead incentivize cyberespionage aimed at acquiring advanced technology information. In this sense, the study reveals a sobering and previously unexamined relationship: cyberespionage is often adopted as a countermeasure to economic sanctions. This is a critical dynamic that policymakers should consider both when designing sanctions regimes and when developing strategies to counter cyberespionage.

In response to the research gap, we argue that export sanctions are not just coincidental to the rise of cyberespionage, but rather constitute a causal driver of it. While cyber operations may proliferate as information technologies advance, our focus lies in showing how economic sanctions systematically incentivize states to adopt cyberespionage as a strategic substitute for accessing restricted technology. Export controls, in particular, are often introduced to impede the flow of advanced technology to (potential) adversaries so as to prevent them from developing sophisticated weapon systems and to maintain technology gaps between sanctioning and sanctioned states. On the other hand, sanctioned countries continue to seek to secure access to advanced technologies not only for national security purposes but also for technological innovation and economic growth. However, since legitimate methods of technology transfer are restricted by export regulations, alternative approaches must be pursued to ensure continuous flows of advanced technology. Therefore, cyberespionage emerges as an attractive policy option for sanctioned states as it can be efficient, difficult to attribute clearly to a particular perpetrator, and allows for plausible deniability.

To test our argument, we conduct both large-N and small-N analyses. For the general trend, we employ a Two-Stage Residual Inclusion (2SRI) approach to address concerns about the endogeneity between economic sanctions and cyberespionage. The results support our hypothesis that states are more likely to conduct cyberespionage under export controls. Countries subject to export sanctions are found to conduct more cyberespionage against sanctioning countries than those not subject to export sanctions, controlling for factors known to influence cyberattacks. The controlled variables, such as strategic rivalry between the two countries and dyadic democracy, are all found to affect

cyberespionage, consistent with predictions from prior research. The case studies focus on North Korea and China, illustrating how they use cyberespionage under export restrictions.

While the discussion on cyberattacks in the context of rivalries has expanded substantially, linking foreign economic policy to a state's malicious behavior in cyberspace remains a relatively new research area and merits further systematic investigation. In light of this, this article is one of the first to identify economic sanctions as a cause of cyberattacks, specifically by establishing a link between export sanctions and cyberespionage. Another contribution the article makes to the literature is that, unlike previous research in the traditional economic sanctions field, which focuses on why the sender state imposes economic sanctions and whether the sanctions succeed or not, this study highlights how the target country responds through cyberspace. The article also makes a policy contribution by cautioning policymakers, who consider economic sanctions, such as export controls, in the context of restricting technology transfer (Reinsch et al. 2024; Meijer 2016). This is noteworthy because such economic measures can provoke countermeasures by the target state in an unexpected domain, such as cyberspace, in the form of cyberespionage to circumvent regulations and gain access to restricted technologies. As export controls on advanced technology are expected to be utilized more extensively in the face of technological competition, the article urges policymakers to consider potential reactions of the target state, which could facilitate the illicit acquisition of restricted technologies through cyberspace.

The remainder of this article proceeds as follows. The next section reviews existing research on cyberespionage in the context of economic sanctions. Then, the article presents the theoretical arguments and derives a hypothesis. This is followed by the research design with data and methodological descriptions, and the large-N and small-N analyses. The conclusion summarizes the findings with discussions of contributions, policy implications, and future research agenda.

CYBERESPIONAGE UNDER ECONOMIC SANCTIONS

Cyberespionage is a burgeoning area of research among International Relations (IR) scholars (Akoto 2024; Lindsay et al. 2015). This trend is partly driven by the rise of cyberspace as a venue where major state actors clash and international norms remain unsettled (Arquilla 2021; Buchanan 2020; Ebert and Maurer 2013; Grigsby 2017; Tikk and Kerttunen 2018). Additionally, cyberespionage

has garnered substantial scholarly attention because it has emerged as a primary method for adversaries to exploit foreign technology, strengthen their national security, and undermine competitors' capabilities.

Cyberespionage in this study refers to the clandestine theft of sensitive information, intellectual property, or state secrets through cyberspace, typically conducted by state-sponsored actors against foreign entities. While often used interchangeably with 'economic espionage' or 'industrial espionage,' it is important to note that industrial espionage generally refers to activities by individual companies against competitors for commercial purposes, whereas economic espionage often encompasses government activities for broader non-commercial or strategic objectives. Our focus here is on state-sponsored cyberespionage aimed at illicitly acquiring technological or strategic information. This form of cyber operation primarily involves unauthorized access and data exfiltration, distinguishing it from cyberattacks aimed at disruption or degradation. It encompasses both short-term espionage, which seeks to gain access to and leverage critical information for immediate advantage, and long-term espionage, which seeks to manipulate an adversary's future decision-making by leveraging gathered information to enhance credibility and capability (Maness et al. 2022).

Despite the growing volume of research on this topic, only a few studies have attempted to systematically identify conditions under which states employ cyberespionage. Many other studies adopt descriptive approaches to cyberespionage in their case studies. Overall, the literature identifies several reasons why states engage in cyberespionage.

First, cyberespionage is a way to promote national security. In their efforts to ensure national security, states traditionally pursue two primary strategies: external and internal balancing. The latter necessarily involves technological development, which is the foundation of both economic and military development. Historically, espionage has been used to exploit foreign technology and secrets that are related to national security (Gilli and Gilli 2018; Glitz and Myersson 2020).

These studies explain the fundamental motivations behind espionage, including in cyberspace. It is true that most states engage in some degree of espionage for national security purposes. However, a comprehensive understanding of the specific conditions under which states are more likely to conduct cyberespionage and why certain states are targeted more than others remains underdeveloped.

Second, and in a similar vein, cyberespionage is often committed between states engaged in strategic and military competition (Choucri and Clark 2018;

Gartzke 2013; Lindsay et al. 2015). Rival states may employ cyberespionage to wreak havoc on the target state. Moreover, when two states are involved in military disputes, cyberattacks may accompany physical collisions on the ground. Alternatively, cyberattacks may serve as a substitute for kinetic weapons to inflict harm on the adversary. As such, states with more cyber capabilities are more likely to employ cyberattacks, including cyberespionage, against their adversaries.

Third, beyond security, the economic structure between the dyads also provides incentives for cyberespionage. Notably, when the target state possesses assets for a perpetrator to steal, it is more likely to experience cyberespionage. The existence of valuable assets to steal can be captured in trade composition. Accordingly, when trade composition between the states is skewed, a state is more likely to steal valuable intellectual properties through cyberspace to make interdependence more symmetrical (Akoto 2021; 2024).

To the best of our knowledge, however, no study has examined the impact of economic sanctions on the incidence of cyberespionage, though a few have addressed the broader relationship between the two. Some of those studies suggest that economic sanctions are imposed because of illicit foreign exploitation of high-tech information. Sanctions are then employed as a strategic response to cyber threats (Lindsay and Cheung 2015). Other studies evaluate the effect of economic sanctions on cyberespionage, although their effectiveness on deterring cyberespionage is debated (Rowe 2019; Rusinova and Martynova 2024). However, this study does not focus on whether economic sanctions are effective. Rather, it seeks to identify the conditions that drive states toward cyberespionage, specifically the role of economic sanctions.

Therefore, this research makes three prominent contributions. First, we offer a new area of research by identifying a previously underexplored link between economic sanctions and cyberespionage. Second, the extant research on cyberespionage, and more broadly cyberattacks, tends to ignore the systematic patterns of the phenomenon, while dealing with it more idiographically. Third, while the economic sanctions literature mostly addresses whether economic sanctions are effective, when economic sanctions are used, and how multilateral sanctions are formed, this study highlights the post-sanctions phase, with particular attention to how targeted states respond through cyberspace following the imposition of economic sanctions.

CYBERESPIONAGE AS A RESPONSE TO ECONOMIC SANCTIONS

Nation-states have a long history of conducting espionage to support international as well as domestic interests. Internationally, when states attempt to achieve internal balancing in the face of security threats, espionage may be pursued in order to steal critical information on diplomatic, defensive, or offensive military strategies and/or technology. States also have domestic incentives because information on technology may serve to uphold regime legitimacy not only through economic development but also through information control capacity, such as internet censorship or cyber surveillance. Some authoritarian states, such as China and Russia, are eager to exploit foreign technologies to maintain social order and prevent challenges from political dissidents (Lindsay and Cheung 2015). As the Internet has spread, cyberespionage has become an alternative method for states to steal crucial information.

Historically, state-sponsored espionage has played a crucial role in smuggling restricted items and stealing information critical to national security (Miller 2022). There are clear incentives for states to engage in exploitation of foreign technology. The "advantage of backwardness" is perhaps the most representative concept that illustrates how less developed states can close military or economic-technology gaps with developed countries (Gerschenkron 1962). By freeriding on the research and development of technology in advanced countries, catching-up states (latecomers?) can save resources that would otherwise have to be spent. The benefits of espionage include not only financial and material aspects of expenses in the technology development process, but also time, know-how, and accumulated experience in design, development, and manufacturing. Thus, innovation is expected to occur more rapidly and efficiently through espionage. As such, technology in high-tech sectors is more valuable to illegally exploit than that of low-tech sectors.

States engage in cyberespionage primarily for two interconnected purposes: national security and economic development/innovation. First, from a national security perspective, states aim to achieve internal balancing against external threats. This inherently involves technological development, which forms the foundation of military strength. When states perceive a technological lag, they may feel threatened within the anarchical international system, viewing it as both a failure of internal balancing and an increased security threat. Therefore, they are motivated to exploit foreign technology and secrets related to national security (Gilli and Gilli 2018; Glitz and Myersson 2020).

Second, concerning economic development and innovation, states seek to close military or economic-technological gaps with more developed countries.

The concept of the "advantage of backwardness" highlights how less developed states can save both time and resources by freeriding on the R&D of advanced nations, thereby accelerating innovation through illicit means. While some argue that increasing technological complexity has reduced this advantage (Gilli and Gilli 2018; Mowery and Rosenberg 1989), the utility of espionage persists, particularly between technologically similar states (Glitz and Myersson 2020), and its expected utility may even increase as the cost of cyber-enabled espionage diminishes.

Economic sanctions, especially export controls, significantly intensify these pre-existing incentives for cyberespionage. Export controls are specifically designed to regulate the outbound flow of high-tech goods, services, and information closely associated with national security. While their effectiveness in impeding technological progress is debated, there is consensus that they can impede access to foreign technology and intellectual property (Jiang 2017) and impose additional costs on obtaining critical items (Fuller 2023; Shivakumar et al. 2024). Consequently, sanctioned states, facing prohibited official access to crucial technological information, become more motivated to acquire it through illicit means. These restrictions on foreign technology hamper their economic and defense innovation, threatening their security. Economic sanctions widen the information gap between states, causing sanctioned states to become concerned about their technological lag (Akoto 2024; Lotrionte 2015). Given the vital role of technological progress in both national security and economic growth, sanctioned states are likely to seek ways to offset this widening gap.

Cyberspace offers an attractive avenue for states to conduct espionage due to its unique characteristics. Cyberespionage is notably cost-efficient as it can be conducted remotely without physical agents or tangible deliveries. It can yield vast amounts of information at a fraction of the cost of traditional espionage, serving as a low-cost substitute for conventional R&D (Melnitzky 2012). Moreover, cyberespionage offers plausible deniability due to the inherent difficulty of attribution. Even if a perpetrator is tracked, state involvement may remain unconfirmed, particularly when proxies are used (Kello 2017, 40; Lachow and Grossman 2018, 393). While customary international law may regard espionage for national security as legitimate intelligence collection (Borghard and Lonergan 2018, 33), the ambiguity of intent and attribution allows governments to deny allegations of illegal cyberespionage, framing it as legitimate intelligence gathering not for commercial purposes. This combination of efficiency, low cost, and deniability makes cyberespionage an appealing countermeasure for sanctioned states seeking to bypass restrictions and acquire denied technologies.

In sum, when economic sanctions prohibit states from accessing technology information, they have higher incentives to conduct espionage for economic development/innovation as well as national security. While cyberespionage may grow alongside general technological development, this study emphasizes that sanctions serve as a strategic push factor—creating material constraints that make cyber operations more appealing. This argument leads to the following hypothesis:

Hypothesis 1: States under export sanctions are more likely to conduct cyberespionage toward states that impose sanctions.

ANALYTICAL FRAMEWORK

We test the argument that espionage is more likely to be conducted when sanctions are imposed to offset the blocked flow of technology information with large-N statistical models, which are then followed by case studies.

Cyberespionage

Data on state-sponsored cyber economic espionage come from the Dyadic Cyber Incident and Campaign Dataset (DCID) version 2.0 compiled by Maness et al. (2022). The dataset distinguishes cyber incidents by three strategies: disruption, espionage, and degradation. Cyberespionage campaigns involve stealing critical information, such as China's theft of Lockheed Martin's F-35 plans. Cyber events such as espionage often occur over long periods of time, and several incidents may overlap during the same period. We add up the total number of cyberespionage incidents undertaken by the sanctioned state recorded in that year.

To analyze more recent time periods and to examine the broader applicability of the hypothesis, this study uses an alternative dependent variable from the European Repository of Cyber Incidents (EuRepoC) Global Dataset of Cyber Incidents (Zettl-Schabath et al. 2025). This dataset includes incidents recorded up to 2024, offering extended temporal coverage. While it does not restrict cases to state-sponsored attacks, it enables the hypothesis to be extended beyond states to domestic actors such as firms, which may also engage in cyberespionage under export sanctions to gain access to advanced technologies. The analysis includes only incidents classified as data theft.

A general caveat should be taken into account when approaching any state intelligence and military operations. For instance, successful cyber economic espionage is typically conducted clandestinely; operations may remain dormant for extended periods before executing their missions at an opportune moment. Even if it is revealed, states tend not to identify themselves as perpetrators of such operations. Furthermore, victims of such attacks—both private firms and government agencies—are often reluctant to disclose these incidents, especially when the damage is significant. Private actors, concerned about stock market reactions and public reputation, have even stronger incentives not to disclose such incidents (Carr 2016). Hence, it is reasonable to assume that a large number of of cyberespionage campaigns remain undisclosed. This could introduce uncertainty bias into the analysis, so the results should be interpreted with these limitations.

Export Sanctions

We use the Global Sanctions Database (GSDB) version 4 for economic sanctions (Felbermayr et al. 2020; Yalcin et al. 2025). Although there are other available sanctions datasets, we use the GSDB because it contains data points up to the most recent year, 2023. Since cyberespionage has only recently emerged as a policy tool of state actors around the 2000s, as reflected in the time span of the DCID, we need to fully leverage the available data without missing observations due to the limited time scope of other variables in our analytical models. Export sanctions measures include export controls, unlike bilateral sanctions measures that include both export and import sanctions, making them the most suitable choice within the dataset. Future research would, however, benefit from data focused exclusively on export controls.

Controls

To address potential endogeneity between cyberespionage and export sanctions, we employ a two-stage approach in which export sanctions are estimated in the first stage, and the resulting residuals are then included in the second stage to correct for endogeneity when estimating cyberespionage.

The first-stage model, predicting export sanctions, includes several key variables. Lagged export sanctions are incorporated to account for the persistence of sanctions over consecutive years. Political affinity between states is measured using dyadic voting alignment scores from the United Nations

General Assembly Voting Data (Bailey et al. 2017), which are claimed to reduce the likelihood of sanctions (Drezner 1999; Drury 2001). We use this indicator instead of other affinity indicators, such as Kendall's tau-b, the S-score, Scott's pi, Cohen's kappa, and alliance data (Chiba 2015; Haege 2011; Signorino 1999; Gibler 2009), due to their limited temporal coverage. To account for the dynamic link between bilateral trade and sanction likelihood (Hafner-Burton and Montgomery 2008; Farrell and Newman 2019), we include the target state's relative trade dependence, calculated from bilateral trade volume (International Monetary Fund 2023) and GDP (United Nations 2024) as a log-transformed difference. Finally, the level of democracy in each dyad, measured by multiplying electoral democracy scores from the V-Dem dataset (Coppedge et al. 2025), is included, as democratic dyads are less likely to impose sanctions on one another (Cox and Drury 2006; Goenner 2007; Hafner-Burton and Montgomery 2008; Lektzian and Souva 2003).

The second-stage model for cyberespionage incorporates several control variables. Lagged cyberespionage is included to account for temporal dependence, as prior incidents can influence future ones. States with stronger cyber capabilities are more likely to employ cyberespionage; thus, the government cyber security capacity index from the V-Dem dataset (Coppedge et al. 2025) is used. To reflect the strategic value of transferable information, we include the dyadic difference in economic complexity, measured by the absolute difference in ECI scores, as cyberespionage is more likely between states with similar industrial structures (Akoto 2024; The Growth Lab at Harvard University 2025). Internet usage, a proxy for digital exposure, is included as the summed and log-transformed rates (International Telecommunication Union 2023). Strategic rivalry, a binary variable from the Strategic Rivalries dataset (Thompson et al. 2021), is included as cyber conflict is more frequent between rivals (Valeriano and Maness 2014). Furthermore, armed conflict, captured by the UCDP Dyadic Dataset (Davies et al. 2024; Harbom et al. 2008) due to MID data's temporal limitations (Palmer et al. 2020), is included as cyberattacks are more likely during conflict. To account for unobserved temporal heterogeneity, the models include year fixed effects, which capture time-specific shocks like technological developments. Unit fixed effects are not included, as they can introduce bias in the presence of dynamic causal relationships (Imai and Kim 2019).

Econometrics

A global sample of states in a directed dyad-year analytical framework over the period 2001-2020 is used, reflecting data availability for key variables. This study analyzes all dyads listed in the Correlates of War (CoW) State System Membership dataset (Correlates of War Project 2017), based on the understanding that cyberattacks can occur regardless of geographic proximity or relative national power. However, to account for potential variations among dyads, results based on politically relevant dyads are also reported for comparison (Lemke and Reed 2001).

This study employs a 2SRI approach to estimate the causal effect of export sanctions on cyberespionage. The 2SRI method is well-suited for addressing endogeneity in nonlinear models (Terza et al. 2008), making it appropriate for this analysis, which examines the relationship between a binary endogenous regressor (**export sanctions**) and a zero-inflated count outcome (**cyberespionage incidents**). In the first stage, export sanctions are estimated using logistic regression. To assess the validity of the instrumental variables, a zero-first-stage test is conducted; the variable Democracy is thus treated as a control variable in the second stage rather than as an instrument. The remaining variables are used as instruments. The second stage employs Poisson Pseudo Maximum Likelihood (PPML) estimation, which incorporates the residuals from the first stage. PPML is preferred over the Negative Binomial (NB) model, which is commonly used for overdispersion, because NB does not accommodate fixed effects reliably unless restrictive assumptions are met (Guimaraes 2008). PPML, by contrast, allows for the inclusion of fixed effects in a more flexible and consistent manner and is robust to heteroskedasticity and an excess of zero observations. For both stages, standard errors are clustered at the dyad level. Missing data are addressed using Multivariate Imputation by Chained Equations (MICE), through which 20 imputed datasets are generated (van Buuren and Groothuis-Oudshoorn 2011). To assess the sensitivity of the results to imputation, additional models are estimated using complete-case analysis, as recommended by prior research highlighting the potential influence of imputation on inference (Lall 2017).

Table 1 summarizes the results of the PPML estimations based on the 2SRI framework, reporting coefficient estimates from six model specifications designed to test the robustness of the relationship between export sanctions and cyberespionage. These models include a naive specification (Model 1), the standard 2SRI model with full controls (Model 2), a specification excluding year fixed effects (Model 3), a model restricted to politically relevant dyads (Model 4), an alternative dependent variable (Model 5), and a complete-case analysis (Model 6).

Table 1. Second Stage PPML

Variables	Model 1 Naive Model	Model 2 Standard Model	Model 3 No Year FE	Model 4 PRD Only	Model 5 Alternative DV	Model 6 Complete Case
Export Sanctions	0.948** (0.334)	0.927* (0.383)	0.798* (0.392)	1.054** (0.397)	0.672** (0.250)	0.940* (0.447)
Residuals		0.201 (0.741)	0.472 (0.837)	0.403 (0.403)	−1.452 (1.115)	0.208 (0.767)
Prior Espionage	0.293*** (0.036)	0.292*** (0.035)	0.268*** (0.041)	0.293*** (0.037)	0.492*** (0.072)	0.301*** (0.036)
Cyber Capacity	1.087*** (0.234)	1.089*** (0.238)	1.099*** (0.241)	0.987*** (0.241)	1.099*** (0.105)	1.064*** (0.258)
ECI Difference	−0.306 (0.232)	−0.302 (0.228)	−0.287 (0.227)	−0.325 (0.228)	−0.240* (0.096)	−0.333 (0.291)
Internet Usage	0.642 (0.453)	0.636 (0.455)	0.684** (0.234)	0.395 (0.432)	0.900*** (0.256)	0.591 (0.460)
Strategic Rivalry	4.937*** (0.453)	4.937*** (0.452)	4.995*** (0.469)	3.412*** (0.443)	3.150*** (0.302)	4.625*** (0.517)
Armed Conflict	1.730 (0.927)	1.718 (0.932)	1.294 (0.977)	2.618** (0.817)	1.577* (0.638)	1.783 (0.931)
Democracy	−2.369** (0.853)	−2.388** (0.860)	−2.360** (0.849)	−2.154** (0.729)	−4.036*** (0.475)	−2.337* (0.976)
Intercept			−11.561*** (1.086)			
Year FE	Yes	Yes	No	Yes	Yes	Yes
Log Likelihood	−1737.5 (−1739.1, −1735.7)	−1737.2 (−1738.8, −1735.5)	−1813.9 (−1815.5, −1812.0)	−1375.5 (−1376.6, −1374.0)	−4343.2 (−4346.8, −4340.0)	−1541.7
Pseudo R2	0.666 (0.666, 0.666)	0.666 (0.666, 0.666)	0.653 (0.653, 0.654)	0.622 (0.621, 0.622)	0.409 (0.408, 0.409)	0.656
imputation	20	20	20	20	20	No
N	711044	711044	747716	68422	788244	510244

***p 〈 0.001; **p 〈 0.01; *p 〈 0.05; Robust standard errors clustered by dyad are reported in parentheses for all models; Pseudo R^2 and log-likelihood are reported as the mean and range across all imputed datasets.

Across all model specifications, the analysis shows that states subject to export sanctions engage in significantly higher levels of cyberespionage against the sanctioning state than those not sanctioned. In Model 2, the presence of export controls increases the expected count of cyberespionage incidents by approximately 153% (exp(0.927) = 2.53), confirming the hypothesis that states subjected to trade restrictions are more likely to target the sanctioning state through cyberespionage. This finding remains remarkably stable even when accounting for fixed effects, restricting the sample to politically relevant dyads (Model 4), or utilizing an alternative dependent variable (Model 5).

The 2SRI framework further allows for a diagnostic check on the endogeneity of sanctions. Notably, the **first-stage residuals** fail to reach statistical significance across all relevant models (Models 2–5). This lack of significance suggests that, within this empirical context, the relationship between export sanctions and cyberespionage is not systematically biased by unobserved time-varying confounders. One plausible explanation is that cyber-related sanctions often target specific entities or individuals via financial freezes, whereas the export controls analyzed here operate at a broader strategic level, mitigating the risk of reverse causality.

The estimates for control variables align with theoretical expectations. **Cyber capacity** and **strategic rivalry** are positively and consistently associated with cyberespionage across all models. **Dyadic democracy**, on the other hand, is negatively associated with cyberespionage, indicating that more democratic pairs of states are less likely to engage in such activities. These findings align with theoretical expectations and existing literature. The conditional significance of other covariates offers further nuance. The **ECI difference** becomes significant only in Model 5, which incorporates non-state-sponsored incidents. This result suggests that narrower technological gaps incentivize industrial espionage, particularly within the private sector, where the marginal utility of stolen intellectual property is higher. Similarly, the impact of internet usage is largely absorbed by year fixed effects in most models, but its significance in Model 5 underscores the critical role of digital infrastructure in facilitating broader cyber-targeting. Finally, the positive effect of armed conflict in Models 4 and 5 indicates that overt kinetic tensions frequently spill over into the cyber domain, particularly when the scope of analysis includes sub-state actors.

Case Studies

The statistical analysis above supports our theoretical argument that sanctioned states are more likely to conduct cyberespionage against the sanctioning state. To demonstrate how the implications of our statistical analysis unfold, we provide case studies of North Korea and China, two of the most prominent examples.

North Korea

North Korea has been subject to export sanctions by at least one country throughout the entire observation period. However, the nature and severity of these sanctions have varied over time. According to the GSDB, sanctions imposed

on North Korea up to 2005 primarily reflect the long-standing unilateral export restrictions initiated by the United States in 1955.

Comprehensive multilateral sanctions began in earnest following North Korea's ballistic missile test in July 2006, which prompted United Nations Security Council Resolution 1695. This resolution condemned the missile launch and called on member states to refrain from transferring missile-related materials, technology, or resources to North Korea (United Nations Security Council 2006). However, its provisions remained relatively limited in scope, with less stringent enforcement than later resolutions.

Until 2012, cyberespionage activities by North Korea were rare. The cyber operations recorded in 2007 and 2008 involved the unauthorized extraction of chemical safety data from South Korea's National Institute of Environmental Research. These early incidents, while involving sensitive information, are not clearly linked to export control measures and are therefore unlikely to reflect a strategic response to sanctions.

However, the tightening of multilateral export controls, particularly after United Nations Security Council Resolution 2094 in 2013, which introduced a 'catch-all' mechanism for restricting dual-use items, coincided with a notable shift (United Nations Security Council 2013). North Korea's leadership explicitly signaled a need to "break through the blockade." This provided a clear strategic context for its subsequent increase in cyberespionage, as such illicit activities offered a pathway to circumvent the denial of critical technologies crucial for national security and economic development.

For instance, North Korean leader Kim Jong-un condemned the sanctions at the March plenary meeting of the Workers' Party of Korea, declaring the need to build an "economic powerhouse" and calling for diversification of external trade to "break through the blockade and create a favorable situation for national economic development" (Korean Central News Agency 2013). These statements indicate that North Korea was actively seeking ways to circumvent export controls and international restrictions.

Concurrently, 2013 marked the beginning of a sharp escalation in North Korea's cyberespionage activities. Between 2013 and 2016, a series of attacks led to the exfiltration of highly sensitive materials, including blueprints for the F-15 fighter jet and internal documents related to nuclear power plants.

In response to North Korea's fourth nuclear test, the United Nations Security Council adopted Resolution 2270 in 2016, which made the previously optional catch-all mechanism mandatory (United Nations Security Council 2016). During the 7th Congress of the Workers' Party of Korea that same year, the North Korean leadership emphasized the principle of "self-reliance first," declaring that

scientific and technological development must be treated as a lifeline in order to overcome the "economic and technological blockade by imperialists" and accelerate national advancement (Korean Central News Agency 2016). These statements suggest a strategic orientation toward using technological innovation to circumvent sanctions and export controls.

Coinciding with this shift, North Korea's cyberespionage activity increased significantly in 2016. In 2016, North Korean operatives breached the networks of domestic defense firms and Daewoo Shipbuilding & Marine Engineering, stealing sensitive technologies related to nuclear delivery systems. Since then, North Korea has continued to engage in broad-spectrum cyber operations targeting financial institutions and cryptocurrency exchanges, including attacks in 2021 on Daewoo Shipbuilding, the Korea Atomic Energy Research Institute, and Korea Aerospace Industries.

Thus, although North Korea has remained under continuous sanctions, the intensity and sophistication of its cyber operations have evolved in response to tightening restrictions. While cyberespionage was rare during the early sanction years following 2006, the imposition of stricter controls in 2013 coincided with a surge in technology-focused espionage. After 2016, North Korea expanded its operations beyond technological theft to include aggressive financial cybercrime, suggesting a shift toward full-spectrum cyber strategies aimed at both resource acquisition and technological advancement.

China

China has been listed in the GSDB as a target of U.S. export sanctions since 2017. However, various forms of U.S. export controls targeting China had been in place well before that date, with changes over time in both scope and intensity. According to the data, China's cyberespionage activity against the U.S. began to rise in 2006. The incidents recorded in 2006 and 2007 primarily involved intrusions into the computer systems of the U.S. Department of State, members of Congress, and high-ranking officials. These early attacks appear to have limited direct connection to export control measures and are therefore not clearly attributable to sanction-related motivations. However, as U.S. export controls began to increasingly target China's access to advanced and dual-use technologies, the strategic implications for China's indigenous innovation capabilities became more pronounced.

In 2007, the United States strengthened its export control regime. President George W. Bush signed the International Emergency Economic Powers Enhancement Act, which amended the 1977 International Emergency Economic

Powers Act to significantly increase civil and criminal penalties for export control violations (U.S. Congress 2007). In parallel, the Bureau of Industry and Security revised export and re-export regulations concerning China (Bureau of Industry and Security 2007). The updated rules required exporters to obtain licenses for certain items that had not previously been restricted, particularly if the exporter knew or had reason to believe the item would be used for military end-use in China. These tightened controls, specifically targeting technologies with potential military applications, created a strategic bottleneck for China's ambition to achieve technological self-sufficiency and enhance its defense capabilities. This policy shift thus provided a clear, albeit unintended, incentive for China to seek alternative avenues for technological acquisition, including illicit cyber means.

Following these regulatory changes, China's cyberespionage activity against the United States escalated noticeably. In 2008, the DCID recorded the first major case of technology-focused cyberespionage attributed to China—Operation SMN, conducted by the Axiom threat actor group (Novetta 2014). Subsequent operations targeted highly sensitive technologies, including data on the F-35 fighter jet (Mount 2009), drone systems (Wong 2013), and a wide array of intellectual property (Department of Justice 2014). By 2013, the group known as APT41 had expanded its activities into the high-tech sector, combining state-aligned objectives with financially motivated intrusions (Mandiant 2019).

In 2016, China's cyberespionage activity against the United States declined significantly according to the DCID. This reduction may be attributed to the September 2015 cybersecurity agreement between U.S. President Barack Obama and Chinese President Xi Jinping, although some skeptics argue this decline reflects a shift in tactics rather than a cessation of activity. The agreement included a mutual commitment by both governments to refrain from engaging in or supporting cyber-enabled theft of intellectual property (The White House 2015). Beginning in 2017, however, the United States initiated a new phase of export sanctions targeting China and began tightening its export control policies. That year, the U.S. government imposed a fine on the Chinese semiconductor firm ZTE for violating Iran-related export sanctions and required the company to implement a three-year export compliance program (Department of Justice 2017). In 2018, export restrictions were imposed on Fujian Jinhua Integrated Circuit Company (Bureau of Industry and Security 2018), and the enactment of the Export Control Reform Act marked a substantial expansion of U.S. controls over emerging and foundational technologies.

Since 2017, China's cyberespionage has increasingly focused on multinational corporations (Sganga 2022) and sensitive military technologies (Volz 2019), while

previously common activities such as the theft of personal data from individuals have notably declined. This shift suggests a reorientation of China's cyber operations following U.S. export control actions. In 2022, the United States further tightened restrictions on advanced semiconductor technologies. In direct response, APT41 reportedly intensified its cyberattacks targeting U.S. semiconductor firms (Montgomery 2025). Overall, the evolving pattern of China's cyberespionage against the United States consistently aligns with the changing scope and intensity of U.S. export controls and sanctions. This alignment demonstrates how a major power strategically adapts its illicit technology acquisition efforts in response to external denial.

CONCLUSION

This article has explored the understudied but increasingly salient relationship between export sanctions and cyberespionage, arguing that economic coercion, particularly in the form of export sanctions, can unintentionally incentivize states to engage in cyber-enabled theft of advanced technologies. Conventionally, economic sanctions are understood as tools for limiting an adversary's technological advancement and strategic capabilities, and are thus intended to discourage illegal activities such as cyberespionage. However, this study demonstrates that such restrictions may inadvertently provoke target states to resort to covert and illicit means—namely, cyberespionage—to acquire the very technologies they are denied through formal channels.

Through both large-N statistical analysis and small-N case studies of China and North Korea, the article provides robust empirical evidence that export sanctions significantly increase the likelihood of cyberespionage by the sanctioned state. These findings suggest that cyberespionage is not merely a function of strategic rivalry or technical capacity, but also a rational response to economic and technological exclusion. States under export control regimes, facing blocked access to critical technologies, may perceive cyberespionage as an efficient, low-cost, and deniable strategy to circumvent restrictions and sustain both developmental and security objectives.

In doing so, this research contributes to both the cyber security and sanctions literature in several important ways. First, it advances our theoretical understanding of cyber behavior by identifying a specific material driver—export sanctions—that shapes states' decisions to conduct cyberespionage.

Second, it moves beyond sender-centric approaches in the sanctions literature by foregrounding the strategic adaptations of target states. Rather than passively absorbing the costs of sanctions, target states actively respond through asymmetric means in cyberspace. Third, this article brings to light the paradox that policies designed to preserve technological superiority may inadvertently erode it by fueling covert and hard-to-detect cyber intrusions.

From a policy perspective, the findings offer a cautionary note for decision-makers designing and implementing export control regimes. While such measures may serve short-term strategic objectives, they also carry the risk of escalating conflict into the cyber domain and encouraging illicit forms of technology acquisition. As export controls are likely to remain a central instrument in contemporary strategic competition—particularly between the United States and its rivals—policymakers must consider the unintended consequences of such tools, including the potential for increased cyber threat activity.

Future research should expand this inquiry by exploring variation across different types of sanctions, sectoral targets, and cyber capabilities of sanctioned states. It should also consider the role of private sector vulnerabilities and international cooperation mechanisms in either mitigating or amplifying the cyberespionage risks associated with economic coercion. In an era in which strategic competition increasingly plays out across both economic and digital frontiers, understanding the interplay between export controls and cyber operations is not only academically pressing but also strategically urgent.

REFERENCES

Akoto, William. 2024. "Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage." *Journal of Peace Research* 61(1): 1-13. https://doi.org/10.1177/00223433231214417

_____. 2021. "International Trade and Cyber Conflict: Decomposing the Effect of Trade on State-Sponsored Cyber Attacks." *Journal of Peace Research* 58(5): 1083–97. https://doi.org/10.1177/0022343320964549

Arquilla, John. 2021. *Bitskrieg: The New Challenge of Cyberwarfare*. Cambridge, UK: Polity Press.

Bailey, Michael A., Anton Strezhnev and Erik Voeten. 2017. "Estimating dynamic state preferences from United Nations voting data." *Journal of Conflict Resolution* 61(2): 430-456. https://doi.org/10.1177/0022002715595700

Blackwill, Robert D. and Jennifer M. Harris. 2016. *War by Other Means: Geoeconomics and Statecraft*. Cambridge, MA: Harvard University Press. https://doi.org/10.2307/j.ctt1c84cr7

Borghard, Erica D. and Shawn W. Lonergan. 2018. "Confidence Building Measures for the Cyber Domain." *Strategic Studies Quarterly* 12(3): 10-49. https://www.jstor.org/stable/26481908

Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press. https://doi.org/10.2307/j.ctv3405w2m

Bureau of Industry and Security. 2007. "Revisions and Clarification of Export and Reexport Controls for the People's Republic of China (PRC); New Authorization Validated End-User; Revision of Import Certificate and PRC End-User Statement Requirements." Accessed at https://www.federalregister.gov/d/E7-11588 (Date of Search : October 6, 2024).

_____ 2018. "Addition of an Entity to the Entity List." Accessed at https://www.federalregister.gov/d/2018-23693 (Date of Search : October 6, 2024).

Carr, Madeline. 2016. "Public-Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92(1): 43-62. https://doi.org/10.1111/1468-2346.12504

Chiba, Daina, Jesse C. Johnson and Brett Ashley Leeds. 2015. "Careful Commitments: Democratic States and Alliance Design." *Journal of Politics* 77(4): 968-982. https://doi.org/10.1086/682074.

Choucri, Nazli and David D. Clark. 2018. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA: MIT Press. https://doi.org/10.7551/mitpress/11334.001.0001.

U.S. Congress. 2007. "S.1612 - 110th Congress (2007-2008): International Emergency Economic Powers Enhancement Act." *Congress.gov* (October 16). Accessed at https://www.congress.gov/bill/110th-congress/senate-bill/1612 (Date of Search : October 6, 2024).

Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Fabio Angiolillo, Michael Bernhard, Agnes Cornell, M. Steven Fish, Linnea Fox, Lisa Gastaldi, Haakon Gjerløw, Adam Glynn, Ana Good God, Sandra Grahn, Allen Hicken, Katrin Kinzelbach, Joshua Krusell, Kyle L. Marquardt, Kelly McMann, Valeriya Mechkova, Juraj Medzihorsky, Natalia Natsika, Anja Neundorf, Pamela Paxton, Daniel Pemstein, Johannes von Romer, Brigitte Seim, Rachel Sigman, Svend-Erik Skaaning, Jeffrey Staton, Aksel Sundstrom, Marcus Tannenberg, Eitan Tzelgov, Yi-ting Wang, Felix Wiebrecht, Tore Wig, Steven Wilson and Daniel Ziblatt. 2025. "V-Dem Country-Year Dataset v15." Varieties of Democracy (V-Dem) Project. https://doi.org/10.23696/vdemds25

Correlates of War Project. 2017. "State System Membership List, v2016." Correlates of War. Accessed at http://correlatesofwar.org (Date of Search : May 29, 2025).

Cox, Dan G. and A. Cooper Drury. 2006. "Democratic Sanctions: Connecting the Democratic Peace and Economic Sanctions." *Journal of Peace Research* 43(6): 709-722. https://doi.org/10.1177/0022343306068104

Cybersecurity and Infrastructure Security Agency. 2024. "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs." Cybersecurity Advisory (July 25). Accessed at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a (Date of Search : August 18, 2024).

Davies, Shawn, Garoun Engström, Therese Pettersson and Magnus Öberg. 2024. "Organized violence 1989-2023, and the prevalence of organized crime groups." *Journal of Peace Research* 61(4): 673-693. https://doi.org/10.1177/00223433241262912

Department of Justice. 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Accessed at https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (Date of Search : May 23, 2025).

_____. 2017. "ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran." Accessed at https://www.justice.gov/opa/pr/zte-corporati

on-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending (Date of Search : October 6, 2024).

Drezner, Daniel W. 1999. *The Sanctions Paradox*. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9780511549366

Drury, A. Cooper. 2001. "Sanctions as Coercive Diplomacy: The U. S. President's Decision to Initiate Economic Sanctions." *Political Research Quarterly* 54(3): 485-508. https://doi.org/10.1177/106591290105400301

Ebert, Hannes and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34(6): 1054-1074. https://doi.org/10.1080/01436597.2013.802502

Farrell, Henry and Abraham L. Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44(1): 42-79. https://doi.org/10.1162/isec_a_00351

Felbermayr, Gabriel, Aleksandra Kirilakha, Constantinos Syropoulos, Erdal Yalcin and Yoto V. Yotov. 2020. "The Global Sanctions Data Base." *European Economic Review* 129. https://doi.org/10.1016/j.euroecorev.2020.103561

Fuller, Douglas. 2023. "Export controls effectively constrain China's advance in microchip production." *DIIS Policy Brief* (August 30). Accessed at https://www.diis.dk/en/research/export-controls-effectively-constrain-chinas-advance-in-microchip-production (Date of Search : May 29, 2024).

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38(2): 41-73. https://doi.org/10.1162/ISEC_a_00136

Gerschenkron, Alexander. 1962. *Economic Backwardness in Historical Perspective*. Cambridge, MA: Belknap Press of Harvard University Press.

Gibler, Douglas M. 2009. *International Military Alliances, 1648-2008*. Washington, DC: CQ Press. https://doi.org/10.4135/9781604265781

Gilli, Andrea and Mauro Gilli. 2018. "Why China Has Not Caught up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage." *International Security* 43(3): 141-189. https://doi.org/10.1162/isec_a_00337

Glitz, Albrecht and Erik Myersson. 2020. "Industrial Espionage and Productivity." *The American Economic Review* 110(4): 1055-1103. https://doi.org/10.1257/aer.20171732

Goenner, Cullen F. 2007. "Economic War and Democratic Peace." *Conflict Management and Peace Science* 24(3): 171-182. https://doi.org/10.1080/07388940701468435

Grigsby, Alex. 2017. "The End of Cyber Norms." *Survival: Global Politics and Strategy* 59(6): 109-122. https://doi.org/10.1080/00396338.2017.1399730

Guimaraes, Paulo. 2008. "The fixed effects negative binomial model revisited." *Economics Letters* 99(1): 63-66. https://doi.org/10.1016/j.econlet.2007.05.030

Haege, Frank M. 2011. "Choice or Circumstance? Adjusting Measures of Foreign Policy Similarity for Chance Agreement." *Political Analysis* 19(3): 287-305. https://doi.org/10.1093/pan/mpr023

Hafner-Burton, Emilie M. and Alexander H. Montgomery. 2008. "The Hegemon's Purse: No Economic Peace between Democracies." *Journal of Peace Research* 45(1): 111-120. https://doi.org/10.1177/0022343307084926

Harbom, Lotta, Erik Melander and Peter Wallensteen. 2008. "Dyadic Dimensions of Armed Conflict, 1946-2007." *Journal of Peace Research* 45(5): 697-710. https://doi.org/10.1177/0022343308094331

Imai, Kosuke and In Song Kim. 2019. "When Should We Use Unit Fixed Effects Regression Models for Causal Inference with Longitudinal Data?" *American Journal of Political Science* 63(2): 467-490. https://doi.org/10.1111/ajps.12417

International Monetary Fund. 2023. "International Trade in Goods (by partner country) (IMTS)." Accessed at https://data.imf.org/en/datasets/IMF.STA:IMTS (Date of Search : May 23, 2025).

International Telecommunication Union. 2023. "Individuals using the Internet." Accessed at https://datahub.itu.int/data/?i=11624 (Date of Search : May 23, 2025).

Jiang, Hui. 2017. "American export control, technology spillover and innovation of Chinese pharmaceutical Industry." *Pakistan journal of pharmaceutical sciences* 30(3): 1151-1155. https://pubmed.ncbi.nlm.nih.gov/28671099

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press. https://doi.org/10.2307/j.ctt1trkjd1

Korean Central News Agency. 2013. "Joseollodongdang Jungangwi 3woljeon wonhoeui Bogo - Rodongsinmun" [Report of the March Plenum of the Central Committee of the Workers' Party of Korea - Rodong Sinmun]. *Korean Central News Agency* (April 2). Accessed at http://www.kcna.co.jp/calendar/2013/04/04-02/2013-0402-011.html (Date of Search : May 29, 2025).

_____. 2016. "Kimjongunje1biseo Joseollodongdang Je7chadaehoe Dangjungangwiwonhoe Saeopchonghwabogo" [Report on the Work of the Party Central Committee at the 7th Congress of the Workers' Party of Korea by First Secretary Kim Jong Un]. *Korean Central News Agency* (May 7). Accessed at http://www.kcna.co.jp/calendar/2016/05/05-07/2016-0507-022.html (Date of Search : May 29, 2025).

Lachow, Irv and Taylor Grossman. 2018. "Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations." In Herbert Lin and Amy Zegart eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Washington, D.C.: Brookings Institution Press, 379-399.

Lall, Ranjit. 2017. "How Multiple Imputation Makes a Difference." *Political Analysis* 24(4): 414-433. https://doi.org/10.1093/pan/mpw020

Lektzian, David and Mark Souva. 2003. "The Economic Peace between Democracies: Economic Sanctions and Domestic Institutions." *Journal of Peace Research* 40(6): 641-660. https://doi.org/10.1177/00223433030406002

Lemke, Douglas and William Reed. 2001. "The Relevance of Politically Relevant Dyads." The *Journal of Conflict Resolution* 45(1): 126-144. https://doi.org/10.1177/0022002701045001006

Lindsay, Jon R. and Tai Ming Cheung. 2015. "From Exploitation to Innovation: Acquisition, Absorption, and Application." In Jon R. Lindsay, Tai Ming Cheung and Derek S. Reverson eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, 51-86. https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

Lotrionte, Catherine. 2015. "Countering State-Sponsored Cyber Economic Espionage under International Law." *North Carolina Journal of International Law and Commercial Regulation* 40(2): 443-541.

Mandiant. 2019. "APT41: A Dual Espionage and Cyber Crime Operation." Accessed at https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation?hl=en (Date of Search : May 20, 2024).

Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Benjamin M. Jensen and Jose M. Macias. 2022. "The Dyadic Cyber Incident and Campaign Dataset, version 2.0." Accessed at https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset (Date of Search : May 20, 2024).

Meijer, Hugo. 2016. *Trading with the Enemy: The Making of US Export Control Policy towards the People's Republic of China*. New York: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190277697.001.0001

Melnitzky, Alexander. 2012. "Defending America against Chinese Cyber Espionage through the Use of Active Defenses." *Cardozo Journal of International & Comparative Law* 20(2): 537-570.

Miller, Chris. 2022. *Chip War: The Fight for the World's Most Critical Technology*. New York: Scribner.

Montgomery, Jim. 2025. "Geopolitical Risks and IP Protection in the Semiconductor Industry." *Electronic Design* (March 13). Accessed at

https://www.electronicdesign.com/resources/industry-insights/article/55274131/intellectual-property-challenges-in-the-semiconductor-industry (Date of Search : May 20, 2025).

Mount, Mike. 2009. "Hackers stole data on Pentagon's newest fighter jet." *CNN* (April 21). Accessed at https://edition.cnn.com/2009/US/04/21/pentagon.hacked/ (Date of Search : May 20, 2025).

Mowery, David C. and Nathan Rosenberg. 1989. *Technology and the Pursuit of Economic Growth*. New York: Cambridge University Press. https://doi.org/10.1017/CBO9780511664441

Novetta. 2014. "Operation SMN: Axiom Threat Actor Group Report." Accessed at https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf (Date of Search : October 6, 2024).

Palmer, Glenn, Roseanne W. McManus, Vito D'Orazio, Michael R. Kenwick, Mikaela Karstens, Chase Bloch, Nick Dietrich, Kayla Kahn, Kellan Ritter and Michael J. Soules. 2020. "The MID5 Dataset, 2011-2014: Procedures, Coding Rules, and Description." *Conflict Management and Peace Science* 39(4): 470-482. https://doi.org/10.1177/0738894221995743

Reinsch, William, Thibault Denamiel and Matthew Schleich. 2024. *Optimizing U.S. Export Controls for Critical and Emerging Technologies: Working with Partners*. Washington, DC: Center for Strategic & International Studies.

Rogin, Josh. 2012. "NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"." *Foreign Policy* (July 9). Accessed at https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history (Date of Search : August 18, 2024).

Rosenbaum, Ron. 2012. "Richard Clarke on Who Was behind the Stuxnet Attack," *Smithsonian Magazine* (April 2012). Accessed at https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516 (Date of Search : May 23, 2025).

Rowe, Brenda I. 2019. "Transnational State-sponsored Cyber Economic Espionage: A Legal Quagmire." *Security Journal* 33(1): 63-82. https://doi.org/10.1057/s41284-019-00197-3

Rusinova, Vera and Ekaterina Martynova. 2024. "Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses." *International Law Review* 57(1): 135-174. https://doi.org/10.1017/S0021223722000255

Schlesinger, Jennifer. 2012. "Chinese Espionage on the Rise in US, Experts Warn." *CNBC* (July 9). Accessed at https://www.cnbc.com/2012/07/09/chinese-espionage-on-the-rise-in-us-experts-warn.html (Date of Search :

July 23, 2025).
Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: Public Affairs.
Sganga, Nicole. 2022. "Chinese hackers took trillions in intellectual property from about 30 multinational companies." *CBS News* (May 4). Accessed at https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies (Date of Search : May 23, 2025).
Shivakumar, Sujai, Charles Wessner and Thomas Howell. 2024. "Balancing the Ledger: Export Controls on U.S. Chip Technology to China." *Center for Strategic and International Studies* (February 21). Accessed at https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china (Date of Search : May 23, 2025).
Signorino, Curtis S. and Jeffrey M. Ritter. 1999. "Tau-b or Not Tau-b: Measuring the Similarity of Foreign Policy Positions." *International Studies Quarterly* 43(1): 115-144. https://doi.org/10.1111/0020-8833.00113
Terza, Joseph V., Anirban Basu and Paun J. Rathouz. 2008. "Two-stage residual inclusion estimation: addressing endogeneity in health econometric modeling." *Journal of health economics* 27(3): 531-543. https://doi.org/10.1016/j.jhealeco.2007.09.009
The Growth Lab at Harvard University. 2025. "International Trade Data (HS, 92)." Harvard Dataverse. https://doi.org/10.7910/DVN/T4CHWJ
The White House. 2015. "FACT SHEET: President Xi Jinping's State Visit to the United States." Accessed at https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States (Date of Search : October 6, 2024).
Thompson, William R., Kentaro Sakuwa and Prashant Hosur Suhas. 2021. *Analyzing Strategic Rivalries in World Politics: Types of Rivalry, Regional Variation, and Escalation/De-escalation*. Singapore: Springer. https://doi.org/10.1007/978-981-16-6671-1
Tikk, Eneken and Mika Kerttunen. 2018. "Parabasis: Cyber-Diplomacy in Stalemate." *NUPI Report* 2018-05. Accessed at http://hdl.handle.net/11250/2569401 (Date of Search : July 23, 2025).
United Nations. 2024. "National Accounts - Analysis of Main Aggregates (AMA)." Accessed at https://unstats.un.org/unsd/snaama (Date of Search : May 23, 2025).
United Nations Security Council. 2006. "Resolution 1695." UN Doc S/RES/1695.
_____. 2013. "Resolution 2094." UN Doc S/RES/2094.
_____. 2016. "Resolution 2270." UN Doc S/RES/2270.

Valeriano, Brandon and Ryan C. Maness. 2014. "The dynamics of cyber conflict between rival antagonists, 2001-11." *Journal of Peace Research* 51(3): 347-360. https://doi.org/10.1177/0022343313518940

van Buuren, Stef and Karin Groothuis-Oudshoorn. 2011. "mice: Multivariate Imputation by Chained Equations in R." *Journal of Statistical Software* 45(3): 1-67. https://doi.org/10.18637/jss.v045.i03

Volz, Dustin. 2019. "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets." *Wall Street Journal* (March 5). Accessed at https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800 (Date of Search : May 20, 2025).

Wong, Edward. 2013. "Hacking U.S. Secrets, China Pushes for Drones." *New York Times* (September 20). Accessed at https://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html (Date of Search : May 20, 2025).

Yalcin, Erdal, Gabriel Felbermayr, Heider Kariem, Aleksandra Kirilakha, Ohyun Kwon, Constantinos Syropoulos and Yoto V. Yotov. 2025. "The Global Sanctions Data Base - Release 4: The Heterogeneous Effects of the Sanctions on Russia." *The World Economy*. https://doi.org/10.1111/twec.13732

Zettl-Schabath, Kerstin, Jakob Bund, Martin Muller, Camille Borrett, Jonas Hemmelskamp, Asaf Alibegovic, Enis Bajra, Alisa Jazxhi, Erik Kellenter, Annika Sachs and Callahan Shelley. 2025. "Global Dataset of Cyber Incidents (1.3.2) Dyadic Dataset." *European Repository of Cyber Incidents*. https://doi.org/10.5281/zenodo.14965395