EPPS 6356: Data Visualization

Final Project

Dr. Ho

Dec. 3, 2025

The Cyber Conflict Globe: Dynamic 3D Visualization of State-Linked Operations, 2005–2023

Jing Tao, Xingyuan Zhao, Eman Ajmal, Tryphosa Htoi San Roi

Introduction

Nation-state cyber operations have become one of the most visible, contentious, and consequential instruments of contemporary international politics. Over the past two decades, the accelerating integration of digital networks into every dimension of economic, political, and social life has created new avenues through which states can pursue strategic objectives. As governments, corporations, militaries, and civil society actors rely increasingly on interconnected systems, the vulnerabilities inherent in these networks have grown more complex and more consequential. Research consistently documents a substantial rise in both the frequency and sophistication of state-linked cyber incidents (Valeriano & Maness, 2015; Gartzke & Lindsay, 2015; Dunn Cavelty, 2024). Empirical tracking supports this trend: estimates from the Council on Foreign Relations (CFR) Cyber Operations Tracker indicate that more than five hundred publicly verified state-sponsored cyber operations occurred between 2005 and 2023, affecting over sixty countries worldwide. Complementary industry assessments report similar patterns. Microsoft's annual threat intelligence analyses demonstrate a sharp escalation in state-sponsored targeting of critical infrastructure, while Mandiant's global threat reports detail persistent infiltration efforts against government agencies, private-sector organizations, and non-governmental institutions.

Taken together, these developments show that cyberspace has evolved into a domain of geopolitical rivalry, coercion, and strategic signaling. Cyber operations now disrupt national security, shape diplomatic behavior, undermine economic resilience, threaten electoral processes, and erode public trust in democratic institutions. As such,

understanding the global distribution, patterns, and evolution of these operations is no longer merely a technical matter it is a fundamental requirement for scholars, analysts, and policymakers engaged in international security.

Motivation: Why Cyber Operations Matter Today

The strategic importance of cyber operations has grown in parallel with increasing global digital interdependence. Nearly all critical infrastructure sectors energy, healthcare, transportation, water systems, and telecommunications depend on vulnerable digital systems that are frequently targeted in state-linked campaigns. High-profile incidents illustrate this transformation. The 2007 attacks on Estonian governmental and financial institutions marked one of the first cases where cyber activity was used as a tool of political coercion. The 2010 Stuxnet worm demonstrated that cyber operations could have tangible physical consequences, sabotaging Iranian nuclear centrifuges in what remains one of the most sophisticated cyber-physical attacks to date. Subsequent breaches of the Ukrainian power grid in 2015 and 2016 revealed the potential for cyber operations to disrupt civilian life during geopolitical crises, while the 2020 SolarWinds infiltration highlighted how supply-chain compromises can simultaneously affect thousands of organizations across multiple continents.

These incidents underscore an important reality: cyber operations operate at the intersection of national security, economic stability, and civic resilience. They are used for espionage, sabotage, coercive bargaining, influence operations, strategic signaling, and crisis manipulation. The covert, deniable, and scalable nature of cyber tools allows states to pursue their objectives while minimizing the risks of open military escalation. Scholars argue that this gray-zone characteristic actions that fall below the threshold of kinetic conflict but still impose meaningful costs has made cyber operations attractive instruments of modern statecraft (Slayton, 2017; Smeets, 2018). In an era of heightened geopolitical tension among major powers such as the United States, China, Russia, Iran, and North Korea, cyber operations have become deeply woven into broader patterns of competition across the diplomatic, economic, and informational spheres.

Theoretical Debates in Cyber Conflict Research

As cyber operations have become more prevalent, academic debates have intensified regarding their conceptualization within international relations theory. Early foundational scholarship debated whether cyberspace constitutes a revolutionary domain that upends traditional strategic logics or whether it represents continuity with long-standing patterns of intelligence, subversion, and state competition (Kello, 2013; Gartzke, 2013; Lindsay,

2013). These debates hinged on the novelty of cyber capabilities: their speed, anonymity, cross-border reach, and ability to produce both symbolic and material effects.

As more empirical evidence accumulated after 2010, the field shifted toward assessing the strategic utility of cyber operations. Scholars questioned whether cyber actions function effectively as tools of coercion, whether they alter crisis escalation dynamics, and how attribution uncertainty shapes their strategic value (Borghard & Lonergan, 2017; Lindsay & Gartzke, 2016; Hodgson et al., 2019). Several incident-based studies argued that cyber operations rarely produce decisive coercive outcomes and generally remain below the threshold of armed conflict (Valeriano & Maness, 2015; Valeriano et al., 2018; Schneider, 2019). According to this perspective, cyber actions are better understood as limited harassment, espionage, or signaling rather than instruments capable of forcing concessions.

A competing perspective suggests that cyber operations should be interpreted within the broader framework of hybrid warfare and great-power rivalry. According to this view, states combine offensive cyber operations with disinformation campaigns, espionage activities, economic coercion, and conventional military posturing to achieve cumulative strategic effects (Valeriano & Jensen, 2019; Whyte, 2018; Lynch, 2024; Foulon, 2024; Dunn Cavelty, 2024). Cyber operations, therefore, cannot be understood in isolation; they form part of integrated campaigns that evolve across multiple domains. These debates highlight a core challenge: despite growing evidence, the field still lacks systematic tools that allow scholars and policymakers to observe how cyber operations unfold across both space and time.

The Gaps in Existing Research and the Need for Improved Visualization

Despite the rapid growth of cyber incident datasets, the tools used to analyze them remain limited. Most published studies rely on static tables, summary counts, or non-interactive geographic maps. While these formats provide aggregate insights, they obscured two crucial dimensions:

1. Temporal variation - when cyber operations escalate, cluster, or correspond with geopolitical events.
2. Spatial distribution - where operations occur, which regions are persistently targeted, and how activities shift over time.

These limitations are not trivial. Cyber operations often occur in waves linked to elections, territorial disputes, sanctions, diplomatic crises, or shifts in foreign policy. Without a dynamic, time-sensitive approach, researchers risk missing the patterns that reveal how cyber operations function within broader geopolitical processes. Prior datasets such as

the Dyadic Cyber Incident and Dispute (DCID) data (Maness et al., 2023) demonstrated that cyber events can be systematically coded, but these databases were not designed for high-resolution visualization.

Contribution of This Project

To address these gaps, this project develops a global, time-animated visualization of nation-state cyber operations using the CFR Cyber Operations Tracker. The CFR dataset, one of the most comprehensive open-source collections of state-linked cyber activity, includes detailed information on sponsors, targets, sectors, operation types, and incident dates. The research design follows a structured sequence: data cleaning, standardization, spatial linking, and integration into a custom 3D visualization.

Incident-level data from 2005 to 2023 are standardized and reorganized into a daily-resolution dataset suitable for temporal filtering. Multi-sponsor and multi-target incidents are separated into unique dyadic records to ensure analytical accuracy. The cleaned data are then joined to global country boundaries using ISO-3 codes, allowing each operation to be mapped spatially.

This combined dataset is embedded within a 3D rotating globe environment created through ArcGIS Scene Viewer and extended via the ArcGIS API for JavaScript. Because Scene Viewer does not natively support automated rotation or synchronized temporal playback, custom scripts were developed to animate both the camera position and the time window. This creates a smooth, self-rotating Earth that "plays" the evolution of cyber operations from 2005 to 2023, providing an immersive visualization of global cyber activity.

Empirical Value: What the Visualization Reveals

The resulting visualization uncovers several important empirical patterns that enrich existing scholarship. Consistent with prior findings, cyber operations are disproportionately concentrated among a small number of major powers, including the United States, China, Russia, Iran, and North Korea (Valeriano & Maness, 2015; Lewis, 2017). Temporal patterns show clear inflection points after 2010 and 2015, supporting arguments about the institutionalization and normalization of offensive cyber capabilities (Kello, 2013; Dunn Cavelty, 2024). Spatial clusters appear across East Asia, the Middle East, and Europe, aligning with geopolitical tensions documented in qualitative case studies (Lindsay, 2013; Kostyuk & Zhukov, 2019).

Beyond these macro patterns, the time-animated design highlights episodic surges linked to political crises, sanctions escalation, military confrontations, and diplomatic disputes. The combination of daily-level temporal resolution and incident-level pop-ups enables

users to move seamlessly from global trends to specific events. In this way, the visualization provides a dynamic, intuitive, and analytically rich perspective on how nation-state cyber operations unfold across space and time.

Data

This study uses data from the Council on Foreign Relations Cyber Operations Tracker, which systematically documents publicly reported nation-state cyber operations from 2005 to 2023. Each entry in the Tracker corresponds to a verified incident identified through publicly available reporting and open-source intelligence assessments. The dataset records the date an incident occurred or was discovered, the country or organization that was targeted, the sponsoring state or actor responsible for the operation, the specific type of cyber activity undertaken, and the sector in which the incident occurred. The sectors represented in the Tracker include government agencies, military institutions, private industry, and civil society organizations. Because the dataset is structured at the incident level, each row represents a single discrete cyber event rather than an aggregated observation. This high-resolution structure enables analyses of both the overall distribution of cyber operations across states and the directional patterns between sponsors and targets.

The raw data required extensive preparation before they could be used for spatial and temporal visualization. The first step was to standardize and convert all date variables into a consistent Date type stored at the daily level, ensuring that the visualization would be able to animate changes with precise temporal fidelity rather than broader, less informative intervals. The second step was to harmonize all country names and convert them into ISO-3 country codes. ArcGIS geographic datasets require standardized country identifiers to match tabular information to spatial polygons, and without ISO coding, many states would fail to join correctly because of inconsistent naming conventions or alternative spellings. The third step was extensive text cleaning across all descriptive fields, including sponsor names, operation types, and affected sectors. This cleaning removed leading or trailing whitespace, corrected inconsistent capitalization, merged duplicate labels, and standardized textual formatting to ensure accurate grouping during visualization.

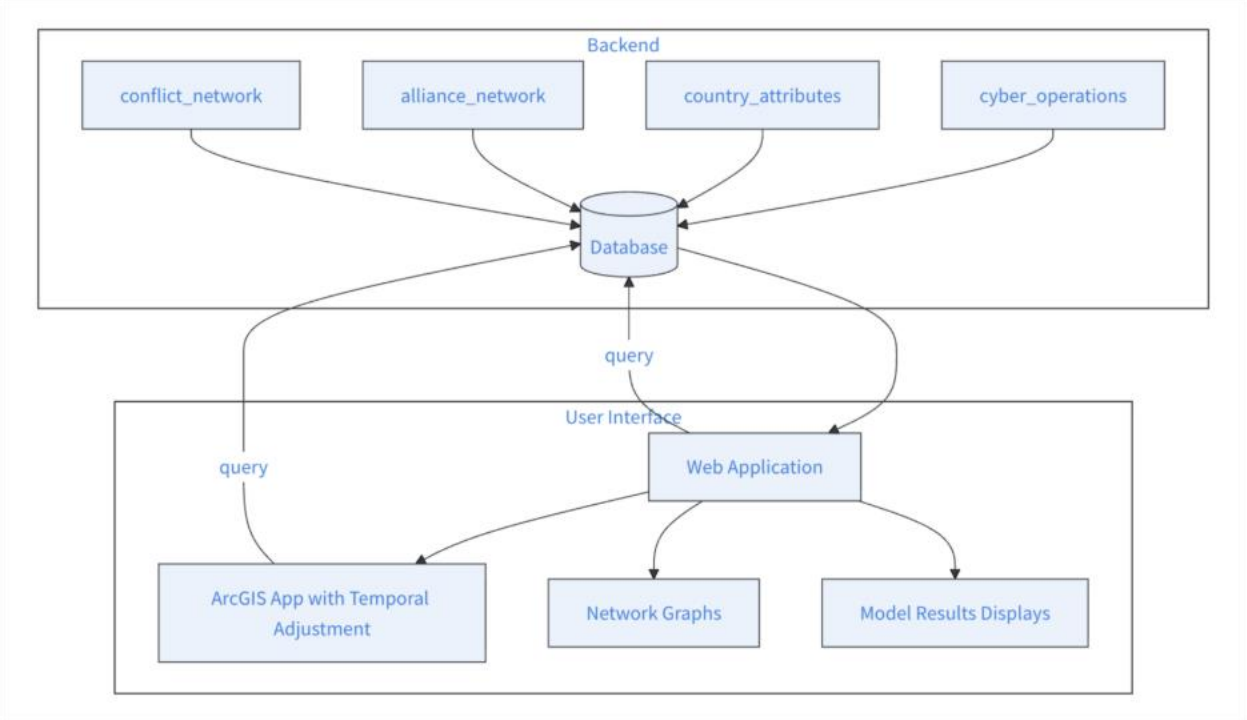
A more complex cleaning procedure was required for records that listed multiple sponsors or multiple targets. In these cases, a single entry was divided into multiple observations so that each record represented a unique sponsor–target pair. This restructuring was necessary to preserve the directional structure of cyber interactions, since failing to

separate these cases would distort both incident counts and dyadic relationships. Duplicate entries created during splitting or during the initial import process were then identified and removed. As a final verification step, aggregated yearly incident totals in the cleaned dataset were compared against official CFR summary tables to ensure no incidents had been inadvertently added or omitted.

A key challenge in the original dataset was classification ambiguity: attacks were often attributed to specific intelligence agencies or military units rather than sponsoring countries, and victims were categorized by sector or organization type without clear geographic mapping. To address this, we employed large language models to systematically extract and annotate country-level identifications from these ambiguous entries, resolving agency-level attributions to their corresponding nation-states and mapping organizational victims to geographic jurisdictions. This LLM-assisted annotation enabled accurate matching to ISO-3 country codes, which was essential for producing reliable spatial visualization.

Only after these procedures did the dataset meet the criteria for producing accurate daily-level temporal animation and spatially consistent mapping. The cleaned dataset provides a robust foundation for generating high-resolution visualizations that reveal both the evolution and geographic distribution of nation-state cyber operations over the eighteen-year period.

Archetecture of the project:



Methods

The visualization was constructed using ArcGIS Scene Viewer and extended through the ArcGIS API for JavaScript to incorporate interactive and animated features that cannot be achieved using Scene Viewer alone. After the cleaned CFR dataset was completed, it was uploaded to ArcGIS Online and joined with a global country boundary layer using ISO-3 country codes. This spatial join created a unified country-level layer, named Joint004, which included both aggregated variables like the total number of cyber operations affecting each state, and all incident-level attributes needed for temporal filtering and pop-up displays. These attributes included the date of each incident, the sponsoring actor responsible for the operation, the affected sector, the type of activity, and descriptive incident summaries.

Within ArcGIS Scene Viewer, the Joint004 layer was symbolized using a continuous red gradient that reflected each state's total number of incidents. Darker shades corresponded to higher incident counts, while lighter shades indicated lower levels of activity. The scene was configured with a Living Atlas world basemap to provide reference boundaries and geographic context beneath the incident layer. The Date field was configured as a time-enabled attribute, which enabled Scene Viewer's time slider to filter incidents based on their recorded dates. This produced a functional 3D WebScene capable of displaying broad spatial and temporal trends. However, Scene Viewer's native

interface imposes two major limitations for dynamic presentations. First, it does not support automatic rotation of a 3D globe, so users must manually drag the map to observe countries in different regions. Second, the time slider cannot autoplay in 3D mode, which prevents continuous temporal animation.

To overcome these limitations, the completed WebScene was embedded into a custom HTML environment through the ArcGIS API for JavaScript. The SceneView component was used to load and render the WebScene with all of its original symbology, configuration settings, and pop-up templates preserved. JavaScript was then employed to add two key dynamic features that transform the WebScene into a fully automated spatial–temporal visualization. The first enhancement was a continuous 360-degree rotation of the Earth. This was achieved by updating the camera's center longitude at a fixed rate within a high-frequency animation loop. As the longitude value increments progressively, the camera appears to orbit the Earth, producing a smooth rotational effect that reveals all world regions in sequence without requiring user interaction. The second enhancement was a custom time-animation script that mimics automatic time-slider progression. This script advances the temporal window in discrete increments and then updates both the SceneView's time extent and the visible slider values. As a result, the visualization simultaneously displays spatial rotation and temporal evolution, offering a synchronized depiction of how global cyber operations unfold over the full eighteen-year period from 2005 to 2023. Beyond rotation and temporal animation, the JavaScript implementation also includes a dashboard-style interface with interactive filters that allow users to subset incidents by year, sponsoring state, or affected sector, along with legends that clarify the symbology and color encoding used throughout the visualization.

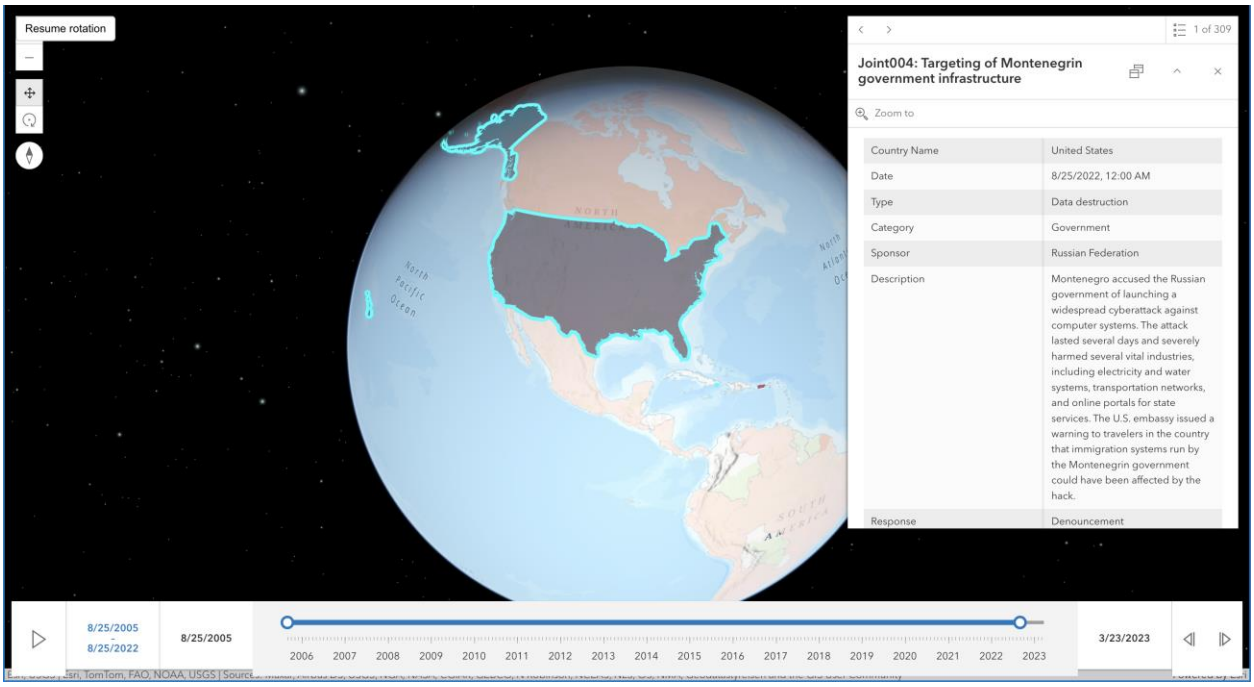
Together, these methods produce a visualization that integrates high-resolution temporal precision with dynamic spatial representation, enabling users to observe cyber operations not as static events but as evolving patterns embedded in global political space.

Data Visualized Results

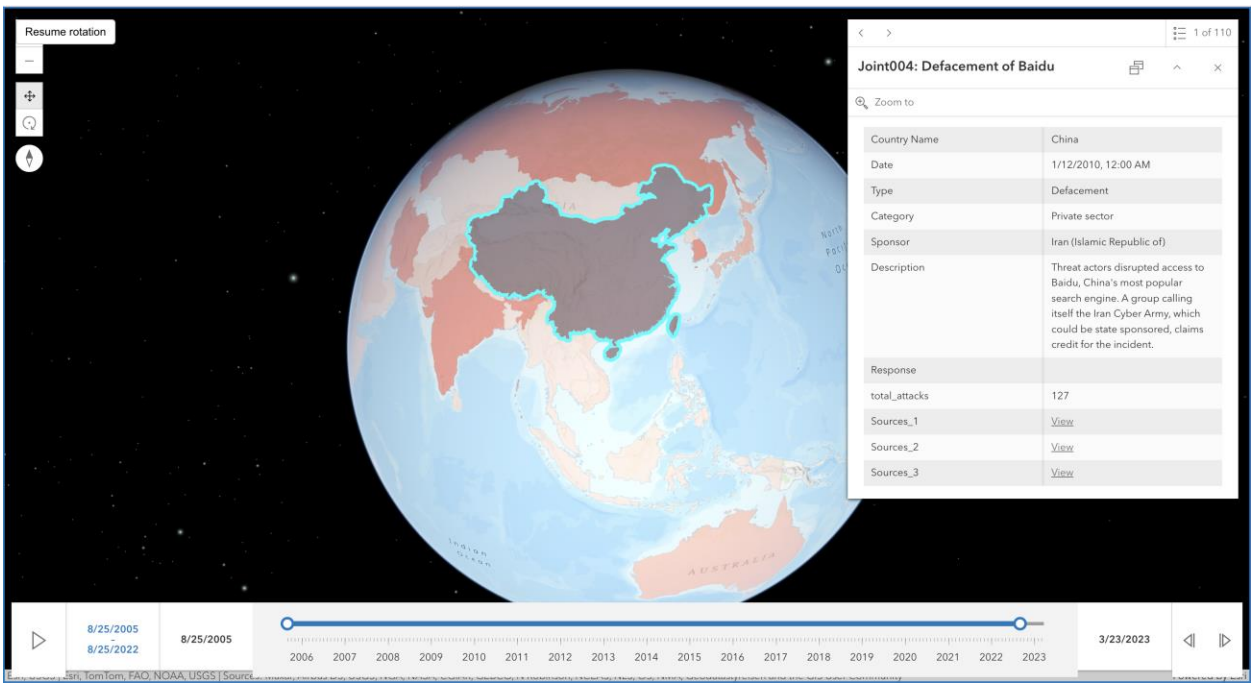
The final visualization takes the form of a fully interactive 3D global map that animates the spatial and temporal patterns of nation-state cyber operations from 2005 to 2023. The Earth appears as a smoothly rendered sphere constructed within ArcGIS Scene Viewer and is enhanced through custom JavaScript scripts that allow it to rotate continuously in a full 360-degree horizontal motion. This automatic and uninterrupted rotation ensures that every region of the world becomes visible without manual user manipulation, allowing viewers to observe how cyber activity is distributed across continents as the globe turns. The countries on the globe are represented as polygon features, and each country’s visual

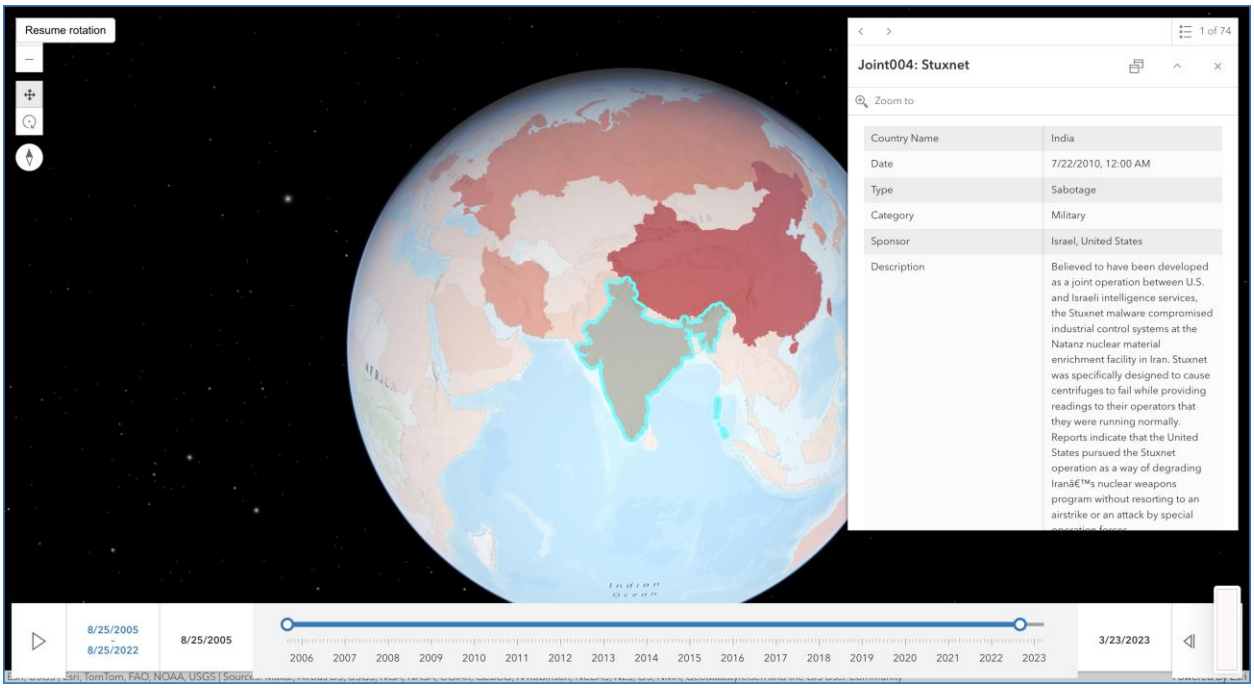
appearance is determined by a quantitative color scale that encodes the total number of cyber incidents attributed to that state. The symbology follows a red intensity gradient in which deeper, darker shades of red represent countries with higher cumulative totals, lighter shades reflect moderate activity, and very pale tones indicate states with few recorded incidents. Countries with no documented incidents appear nearly unshaded, creating an intuitive visual hierarchy of global cyber exposure.

Using the cleaned CFR dataset, the numerical distribution of cyber incidents produces clear and empirically grounded patterns on the globe. The United States stands out as the darkest and most prominent state, with 321 documented cyber incidents, making it the country with the highest overall exposure in the entire dataset.



The next most affected country is China, with 127 incidents, followed by a cluster of significantly targeted states including Ukraine (92), Russia (84), South Korea (83), India (78), the United Kingdom (75), Germany (72), and Iran (72). These countries consistently appear in darker shades of red across the visualization and form the core geographic concentration of cyber operations.





A second tier of moderately targeted states includes Israel (56), Japan (55), Australia (44), Canada (42), France (40), and Pakistan (35), each represented with medium-saturation tones that indicate meaningful but comparatively lower activity levels. A third category consists of lightly targeted states such as Vietnam (28), Poland (27), North Korea (26), Turkey (26), the Netherlands (23), Afghanistan (22), Switzerland (22), Hong Kong (21), and others, which appear in pale red tones. This color-based encoding not only reflects the

underlying data with precision but also allows the viewer to grasp global disparities in cyber activity at a glance.

A central component of the visualization is the time slider positioned at the bottom of the interface. This slider animates the evolution of cyber operations by automatically advancing the temporal window from 2005 to 2023. At any given moment, the slider determines which incidents appear on the map. As it progresses forward, the shading of each country dynamically updates: states darken when incidents fall within the active time window and lighten when earlier incidents no longer meet the temporal criteria. This creates a fluid temporal–spatial effect in which cyber activity visibly expands, contracts, or shifts across regions. The visualization reveals a gradual rise in global cyber activity after 2010, followed by a sharper increase after 2015. Several countries, such as Ukraine, display notable spikes during specific geopolitical periods. Because the dataset stores dates at the daily level, these changes appear with high temporal precision, enabling viewers to distinguish between sustained periods of cyber activity and short bursts of intense incidents.

In addition to color shading, each country is automatically labeled with the date of its most recent cyber incident within the selected time window. This label changes dynamically as the slider advances. For example, if a country experienced its most recent attack in 2021, the map displays “2021” during the relevant stage of the animation. This dual encoding—color representing total exposure and the label representing recency—allows viewers to compare long-term vulnerability with short-term activity simultaneously. As the time slider moves, these labels continuously update, highlighting which states have recently experienced cyber operations and which have not.

The continuous rotation of the Earth is achieved through a JavaScript-controlled camera movement that adjusts the global longitude at a fixed rate. This method creates a smooth orbital trajectory in which the camera sweeps across the Americas, moves toward Europe and Africa, transitions through the Middle East and Asia, and finally returns across the Pacific. The rotation speed and tilt are calibrated to maintain a stable viewing angle, ensuring that all countries receive equal visibility throughout the animation cycle. When combined with the time slider’s progression, this rotation allows viewers to observe how cyber operations cluster within regions and how these patterns evolve over nearly two decades. For instance, certain regions darken simultaneously during periods of heightened geopolitical tension, while other states exhibit isolated bursts of incidents that fade as the timeline advances.

Despite its automated features, the visualization remains fully interactive. When a viewer clicks on any country, a detailed pop-up panel appears, containing incident-level information drawn directly from the CFR Cyber Operations Tracker. The panel lists the date of the cyber operation, the sponsoring actor responsible for the incident, the target organization or country, the type of cyber operation (such as espionage, disruptive attacks, data theft, or infrastructure interference), the sector affected (including government, military, private industry, or civil society), and a descriptive note summarizing the event. This interactive element allows users to transition seamlessly between macro-level global patterns and micro-level incident narratives and to examine the specific characteristics of any cyber operation in detail.

Overall, the visualization operates as a comprehensive and empirically grounded spatial–temporal representation of global cyber activity from 2005 to 2023. Through its integration of cumulative color encoding, recency labels, automated temporal animation, and continuous global rotation, the visualization illuminates persistent hotspots, emerging areas of cyber conflict, and long-term structural shifts in the geography of nation-state cyber operations. Its combination of spatial detail, temporal precision, and interactive depth provides a powerful analytical tool for identifying where, when, and how cyber operations unfold across the international system.

Conclusion

This project developed a global, time-animated 3D visualization of nation-state cyber operations using the Council on Foreign Relations Cyber Operations Tracker from 2005 to 2023. After extensive data cleaning including harmonizing dates, standardizing ISO-3 country codes, splitting multi-sponsor and multi-target incidents, and removing duplicates the cleaned incident-level dataset was merged with global country boundaries in ArcGIS Online. We then used ArcGIS Scene Viewer and customized JavaScript scripts to produce an automated, rotating 3D globe with synchronized temporal animation. The results revealed clear empirical patterns: cyber operations are highly concentrated among a small set of major powers (the United States, China, Russia, Iran, and North Korea), global activity accelerates rapidly after 2010 and intensifies after 2015, and regional clusters emerge around East Asia, the Middle East, and parts of Europe. The animated visualization also shows episodic surges during political crises and demonstrates how cyber conflict evolves as a dynamic global system rather than isolated, static incidents.

Significance of Results and Policy Implications

For policymakers, security experts, and international relations, this visualization benefits a lot because we can actually see when and where cyber operations cluster, which makes it easier to spot hotspots and predict when things might heat up. That means governments can react faster, focus their defenses, and hopefully avoid getting caught off guard. The tool also shows just how much countries are investing in offensive cyber capabilities. it's not a passing trend; it's part of their long-term strategy now. That reality pushes the case for tougher global rules, better ways to figure out who's behind attacks, and more cooperation between countries to keep things from spiraling. This visualization serves a good tool to make smarter, evidence-based decisions and build better early-warning systems.

Data Limitations and External Validity

Despite its analytical value, the CFR Cyber Operations Tracker dataset carries limitations that shape the external validity of our findings. The dataset reflects only publicly reported and verified cyber incidents, meaning that covert, unreported, or classified operations (a substantial portion of real cyber activity) are not included. Reporting biases also vary by country: democratic states with free media tend to disclose incidents more frequently, while authoritarian governments may suppress information, producing systematic undercounting in some regions. Additionally, attribution remains a fundamental challenge in cyber research; many incidents cannot be conclusively linked to a specific state actor, and misattribution can distort geographic patterns. Because the dataset captures only the date of discovery or reporting, rather than the exact date of compromise, temporal patterns may not perfectly reflect operational timelines. These constraints limit generalizability and caution against oversimplifying causal claims based solely on visual patterns.

Extensions for Future Research

Future research works can build on this project in several directions. Technically, the visualization can be expanded by incorporating severity metrics, economic impact estimates, or indicators of operational sophistication to provide more nuanced distinctions between incident types. Methodologically, machine-learning classification or anomaly-detection techniques could be integrated to predict where cyber operations are likely to emerge next. Spatially, future work could adopt network-based visualizations that highlight directional sponsor–target relationships or map cyber operations alongside other instruments of hybrid warfare such as disinformation campaigns. The visualization could also be extended into an interactive dashboard that includes filters for sector, operation type, or individual sponsoring states. Finally, combining CFR data with alternative datasets

such as Mandiant reports, Microsoft threat intelligence, or the DCID dataset would enhance robustness and provide multi-source triangulation of global cyber conflict trends.

References

Borghard, E. D., & Lonergan, S. (2017). Cyber operations as imperfect tools of coercion. International Security, 41(3), 7–51.

https://doi.org/10.1162/ISEC_a_00267

Dunn Cavelty, M. (2024). The Politics of Cyber-Security (1st ed.). Routledge. https://doi.org/10.4324/9781003497080

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. Contemporary Security Policy, 45(3), 426-458. https://doi.org/10.1080/13523260.2024.2365062

Gartzke, E. (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

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: offense, defense, and deception in cyberspace. Security Studies, 24(2), 316-348. https://doi.org/10.1080/09636412.2015.1038188

Panda, S., Woods, D. W., Laszka, A., Fielder, A., & Panaousis, E. (2019). Post-incident audits on cyber insurance discounts. Computers & Security, 87, 101593. https://doi.org/10.1016/j.cose.2019.101593

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7–40.

https://doi.org/10.1162/ISEC_a_00138

Kostyuk, N., & Zhukov, Y. (2019). Invisible digital front: Can cyberattacks shape battlefield events? Journal of Conflict Resolution, 63(2), 317–347.

https://doi.org/10.1177/0022002717737138

Lewis, J. A. (2018). Rethinking cybersecurity: strategy, mass effect, and states. Rowman & Littlefield.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404.

https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R., & Gartzke, E. (2018). Coercion through cyberspace: the stability-instability paradox revisited. Coercion: The Power to Hurt in International Politics, 179-203.

Lynch, T. F. (2024). Forward Persistence in Great Power Cyber Competition. The Cyber Defense Review, 9(3), 81-103. https://www.jstor.org/stable/48836260

Benson, M. (2022). Towards a Research Guide for Cyber Threat Intelligence (Master's thesis, Utica University).

Microsoft. (2022). Microsoft Digital Defense Report.

https://www.microsoft.com/security/blog/microsoft-digital-defense-report/

Shandler, R. (2025). Cyber Conflict & Domestic Audience Costs. International Interactions, 1-25. https://doi.org/10.1080/03050629.2025.2478145

Slayton, R. (2016). What is the cyber offense-defense balance? Conceptions, causes, and assessment. International Security, 41(3), 72-109. https://doi.org/10.1162/ISEC_a_00267

Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. Journal of Strategic Studies, 41(1–2), 6–32.

https://doi.org/10.1080/01402390.2017.1288107

Valeriano, B., & Jensen, B. (2019). The information contest in cyberspace. Texas National Security Review, 2(3), 37–56.

https://tnsr.org/2019/05/the-information-contest-in-cyberspace/

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.

https://global.oup.com/academic/product/cyber-war-versus-cyber-realities-9780190204792

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). Cyber strategy: The evolving character of power and coercion. Oxford University Press.

Cunliffe, K. S. (2021). An Existential Crisis and a Golden Opportunity?: Assessing Hard-target Espionage in the Cyber Era (Doctoral dissertation, Aberystwyth University).