# Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 2.0

**Ryan C. Maness, Brandon Valeriano, Kathryn Hedgecock, Benjamin M. Jensen and Jose M. Macias**

**July 2022**

**Suggested Citation:**
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,* available at: https://drryanmaness.wixsite.com/cyberconflcit/cyber-conflict-dataset

## Overview

This codebook presents a point of reference for variables for dyadic rival states that are in Dyadic Cyber Incident and Campaign Dataset (DCID) version 2.0 for the years 2000-2020. This builds upon on the previous version 1.0 released by Valeriano and Maness (2014, 2015), version 1.1 released by Maness, Valeriano, and Jensen (2017), and version 1.5 for the years 2000-2016 (Maness, Valeriano, and Jensen 2019).

The DCID is primarily focused on rivals for data construction purposes, simplifying the complicated process of identifying cyber events. This dataset can be modified in many ways, including removing the dyadic component to make it monadic. Here we are focused on observable incidents and campaigns between international nation-states as interactions between criminal elements and other non-state actors would require different data collection strategies and theories.

Rival dyads are extracted from the Klein, Diehl and Goertz (2006) enduring rival dataset as well as Thompson's (2001) strategic rival dataset. Each pair of states engaged in cyber conflict has two states involved, on opposite sides of the cyber incidents and campaigns. We do add certain dyads that are not necessarily rivals according to the Klein et. al. criteria but have significant cyber interactions, such as Russia-Estonia, Russia-Ukraine (until 2014), and China-Taiwan.

For individual cyber conflicts, we use the phrase 'cyber incident.' Incidents may include thousands of events, but accounting for every single intrusion or attack made is impossible and unwieldy. As Healey (2021) asks, "should the Russian intrusion into SolarWinds be coded as a single campaign, an active intrusion into 110 organizations or a latent intrusion into 10,000?"[1] The answer is obvious based on how a dataset is constructed, SolarWinds is but one incident that can be decoupled at will into its individual components or added with other incidents to denote a campaign, there is no need to make that choice at this stage and we leave it up the researcher.

Using select variables from the Integrated Crisis Early Warning System (ICEWS) events dataset (Boschee et. al. 2015), for a series of cyber incidents and conventional foreign policy actions (diplomatic, economic, military) between two states over a limited period of time, we use the term 'cyber campaigns.' This appendix pertains to the description of coding efforts for these individual cyber events as well as the coding for the events captured in the cyber campaign dataset.

[1] Jason Healey, Understanding the Offense's Systemwide Advantage in Cyberspace 12/22/2021, https://www.lawfareblog.com/understanding-offenses-systemwide-advantage-cyberspace

For the coding of the variables for all pairs of states added to the dataset (non-state actors or entities can be targets but not initiators as long as they critical to state based systems, or if the original hack escalates into an international incident in the non-cyber domain), the initiation must come from a government or there must be evidence that an incident or campaign was explicitly government sanctioned (see below for responsibility confirmation). For the target state, the object must be a government entity, either military or non-military; or a private entity that is part of the target state's national security apparatus (power grids, defense contractors, and security companies), an important media organization (fourth estate), or a critical corporation (banks, retail giants, automakers, etc.). The dataset does not include multilateral cyber incidents; these types of incidents are only coded at the dyadic level. Third parties are noted and coded as an additional variable in the data.

Version 1.0 of DCID uncovered 126 active rival dyads in the data (Valeriano and Maness 2014, 2015). Valeriano and Maness (2014) identified 110 cyber incidents within 45 overall disputes among 20 of the 126 pairs of states. Version 1.1 (Maness, Valeriano, and Jensen 2017) expanded to 192 incidents within multiple disputes from the years 2000-2014. It includes new variables and coding methods, as well as expanding the inclusiveness of relevant non-state targets to include national security contractors, media organizations, and other relevant corporations such as banks, technology companies (Google, Apple), and utility companies for the years 2000 to 2014. We do not code non-state initiators in this dataset; the initiators must be state entities. Groups such as the Syrian Electronic Army, cyber-jihadists such as the Islamic State, or hacktivist groups such as Anonymous are not included as this would expand the purpose and scope of this data beyond measure.

Version 1.5 builds upon the efforts of version 1.1 and adds a new variables and greater context to cyber conflict at the nation-state level. One added variable to the updated version captures information warfare that is cyber-enabled, which we call cyber-enabled information operations (CIO). CIOs are state based actions, in the context of an ongoing cyber action, seeking to communicate a message or manipulate the reception of digital information for malicious purposes among a targeted population. The actions are intended to sow discontent, change policy direction, or serve as a warning to an adversary in digital space. The political warfare launched by Russia against the United States during the 2016 presidential election, which included cyber and disinformation operations, is a primary example of capturing this variable in the dataset.

Version 2.0 has added new variables of relevance and has also dropped several variables that were recorded in previous dataset. We have recorded 429 incidents for this current version. As the popular, academic, and practitioner lexicons regarding advanced persistent threats (APTs) has led to there being no formal definition, we discarded the variable due to the term's lack of fidelity. Another dropped variable is the interaction type variable (offense, defense, nuisance) as this variable is better captured by the "cyber objective" variable that was added in version 1.1. We have also dropped the "government statement" variable from this iteration, as there is not enough staffing currently available to accurately record these phenomena. The final variable that has been eliminated from the updated dataset are the "third-party target" variable.

Three new variables that have been added to DCID 2.0 include critical infrastructure, supply chain cyber incidents, and ransomware incidents. The "critical infrastructure" variable uses the U.S. Department of Homeland Security's (DHS) 16 different sectors that it considers critical infrastructure to the United States (see https://www.cisa.gov/critical-infrastructure-sectors for more details). Next is the supply chain variable, which codes the presence or absence of a targeted supply chain operation in the cyber domain. Finally, the ransomware variable looks at whether or not the target was digitally locked out of its data access for a ransom payment, and this cyber operation was initiated by a state actor.

In lieu of cyber disputes (see Valeriano and Maness 2014, Maness, Valeriano, and Jensen 2017) from past versions of the DCID, version 1.5 and the updated 2.0 has added a cyber campaigns sheet to the current version of international cases. Cyber campaigns assume that cyber operations do not happen in isolation, and that states often times use diplomatic, economic, and military instruments of power and leverage in tandem with cyber operations, for either coercive effect or to alter the balance of information with its rival through manipulation or disruptive strategies (Valeriano, Jensen, and Maness 2018). These variables that capture these conventional foreign policy tactics are represented in the new campaigns dataset are extracted from the ICEWS events dataset. Only certain thresholds of events and their subsequent intensity, of which are established through conflict-cooperation scores by the Conflict and Mediation Event Observations (CAMEO) scale (Schrodt 2012), are coded into the campaign dataset. CAMEO scores are modeled after the Goldstein (1992) conflict-cooperation scale for the World Event Interaction Survey (WEIS) data and updated for the ICEWS dataset. This scale is interval and ranges from scores of -10 and 10, with the more negative the score the more intense the conflict between actors, and the more positive scores capturing the level of intensity of cooperation between actors. Details of which variables extracted from ICEWS and the threshold of events scores are described below.

The final new variable captures campaign severity and is an interval intensity score much like those captured with CAMEO or Goldstein scores for conventional event intensity. We capture campaign severity by adding up all of the CAMEO scores based on the number, intensity (positive or negative) and type of conventional foreign policy action (diplomatic, economic, military) coded for each event. Specific coding procedures for campaign severity are described in detail below.

## Specific Procedures

The Cyber Conflict Data Project was developed to produce replicable and reliable dataset for all cyber incidents and campaigns between states and relevant non-state targets. The coding method begins with the Correlates of War (COW) foundational procedures in examining sources throughout history, in the media, and, new for cyber conflict, from government or critical cyber security firm reports.

An example the Militarized Interstate Disputes (MID) collection, which records cases of conflict between states "in which the threat, display or use of military force short of war by one member state is explicitly directed towards the government, official representatives, official forces, property, or territory of another state" (Jones, Bremer, and Singer 1996). It uses historical and diplomatic sources to isolate and codify each isolated incident.[2]

Cyber conflict is a more recent phenomenon than militarized disputes, as we demark the beginning of widespread international cyber conflict to begin with the year 2000, after the Y2K crisis. We are able to access information on cyber incidents and disputes using search engines as our uniform data extraction tool, as well as the other sources mentioned. In the future, automatic

[2] Other conflict dataset examples that inspired this collection are Upsala: https://ucdp.uu.se/ and PRIO: https://www.prio.org/Data/

events data searches may be undertaken but for now we are confident we can maintain an active dataset using focused search methods, mostly recently with an army of intern coders.

For the purposes of this study, electromagnetic pulses (EMPs), radar jamming, laser jamming/deception, and other measures/countermeasures traditionally considered electronic warfare (EW) are not defined as cyber incidents. Cyber incidents require the manipulation of computer code for malicious purposes. Electronic manipulation either damage or destroy circuitry through electronic (i.e., radio waves) and/or directed energy. We focus on cyber conflict as the manipulation of code through networks.

We focus on the following search terms to start our investigation. These search parameters are not exclusive, and the coder should endeavor to examine computer security reports and government information after incidents are identified to aid in coding the supplemental variables. In a search engine, enter "participant A e.g. Iran" AND "participant B e.g. Israel" AND "cyber" OR "internet attack" OR "infrastructure attack" OR "government cyber-attack" OR “network breach” OR “hack” and customize the date range for 1/1/2000 to 12/31/2020.

After an incident is identified, computer security firm reports (Kaspersky, McAfee, Symantec, CrowdStrike, Mandiant, among many) and government reports (ODNI, FBI, DHS, DoJ indictments, among many) are used to further code each incident. The following is advice we provide to coders to guide their efforts in data collection.

## Variables for the Dyadic Cyber Incident and Campaigns (DCID) Dataset, Version 2.0 Incident Sheet

A. Cyber incident number (decided by dyad pair number and then earliest start date)
B. Dyad pair (combined COW country codes)
C. State A (first state in the dyad by lowest COW country code)
D. State B (second state in the dyad by higher COW country code)
E. Name of cyber incident
F. Incident Start Date (either specific date if available, accurate to the month otherwise)
G. Incident End Date (either specific date if available, accurate to the month otherwise, end date usually is when an incident is made public or eradicated by the target, or both)
H. Method of interaction/incident, 1-4 with decimal denotations for infiltrations (methods are listed below) for incidents: defacements are vandalism; DDoS, zombies, botnets, and the like will be denial of service; any incident that uses spear phishing will be an intrusion, which includes Trojans, trapdoors, spear-phishing techniques, and backdoors. Intrusions are used in most theft/espionage operations; infiltrations, are malware that is usually worms or viruses, but can also be logic bombs and keystroke logs.
I. The type of target (private/non-state, government non-military, government military)
J. The initiator of the interaction (COW country code)
K. The specific coercive strategy of the cyber incident (disruption, short or long-term espionage, degradation)
L. Whether or not an information operation was used as a result of the cyber incident
M. Whether or not the incident successfully achieved its objective; did it breach the target’s network and fulfill its intended purpose
N. Whether or not the political objective evoked a concessionary change in behavior of the target state.

O. Whether or not a third party was involved in the initiation (other state, rebel group, corporation) 1 = yes, 0 = no; Sometimes, but not often, third party states will be involved in the initiation of a cyber incident. Look for explicit evidence that a third party was involved. Israel was a part of the United States' Stuxnet operation, for example.
P. Severity level on the 0-10 scale level, given below for both incidents and campaigns
Q. Damage type (1. Direct and immediate, 2. Direct and delayed, 3. Indirect and immediate, 4. Indirect and delayed)
R. Critical infrastructure sector (1-17): see https://www.cisa.gov/critical-infrastructure-sectors
S. Supply Chain (1 for "yes", 0 for "no")
T. Ransomware (1 for "yes", 0 for "no")
U. Stated or interpreted strategic/political objective of the cyber incident
V. Key sources for the cyber incident

Once these procedures are finished, responsibility is the next and very important step in the coding process. To verify that the initiator was in fact the government or a government-sanctioned activity (use of proxies, mercenaries, or private industry to act on behalf of a state), the coding process goes through another process of verification. Attribution of cyber incidents can be a problematic issue; therefore, we focus on what is called responsibility (Goodman 2010:128). One of the advantages of a cyber incident is deniability. In this dataset, states that use information warfare must be fairly explicit and evident. If the responsibility of an incident is in serious doubt, we do not code it as a state-based action. We do not take conventional wisdom at its word for operations and instead analyze the history of relations, the intent of the action, likelihood of government complacency and code disputes from this perspective. Therefore, simple news stories extracted by search engines such as "Google News" are not enough to make the dataset. Responsibility must be verified by government statements, policy reports, internet security firm reports, white papers from software security firms (Symantec, McAfee, Kaspersky), or cyber-security agency sources.

**Coding for cyber incidents:** For individual cyber conflicts, we use the phrase 'cyber incident.' Incidents such as ShadyRat include thousands of intrusions, but accounting for every single intrusion the operation made is impossible and unwieldy. Therefore, ShadyRat and other multiple-intrusive incidents are coded as just one incident per dyad as long as the goals and perpetrators remain stable. Each cyber incident is directed by one state or on behalf of the state against another state or state's national security apparatus, media outlets, or relevant multinational corporations.

## I. Methods of cyber incidents

Many news sources will report cyber incidents as viruses, because they do not have the technical know-how to categorize these types of interactions. It is important that coders are aware of this and make sure to code these incidents properly by finding additional reports. The news search is the primer to find cyber incidents; the latter documents are what you will need to code these incidents properly.

1. Vandalism: Website defacements, propaganda: Hackers use SQL injection or cross-site scripting (forms of command code) to deface or destroy victims' web pages. Although rather benign, these attacks may have important psychological effects.

2. <u>Denial of Service, DDoS, Botnets</u>: distributed denial of service: DDoS attacks flood particular Internet sites, servers, or routers with more requests for data than the site can respond to or process. The effect of such an attack effectively shuts down the site thus preventing access or usage. Government sites important to the functioning of governance are therefore disrupted until the flooding is stopped or the attackers disperse. Such attacks are coordinated through "botnets," or a network of computers that have been forced to operate on the commands of an unauthorized remote user. The primary impact of DDoS attacks via botnets is the temporary disruption of service.
3. <u>Network Intrusion:</u> "Trapdoors" or "Trojans" and Backdoors: Trapdoors or Trojans are unauthorized software added to a program to allow entry into a victim's network or software program to permit future access to a site once it has been initially attacked. The purpose of trapdoors is to steal sensitive information from secured sites. Spear phishing is utilized to inject these cyber methods into networks. Here the initiator sends emails to employees or contractors of the targeted network, and if the email is opened, the intrusion is introduced to the system. The botnet technique is another option where a human being injects the intrusion from a portable drive such as a USB or disk.
4. <u>Network Infiltration:</u> Examples of attacks include logic bombs, viruses, packet sniffers, and keystroke logging. These methods force computers or networks to undertake tasks that they would normally not undertake. 1) Logic bombs are programs that cause a system or network to shut down and/or erase all data within that system or network. 2) Viruses are programs which attach themselves to existing programs in a network and replicate themselves with the intention of corrupting or modifying files. 3) Worms are essentially the same as viruses, except they do not need to attach themselves to existing programs. 4) Keystroke logging is the process of tracking the keys being used on a computer so that the input can be replicated in order for a hacker to infiltrate secure parts of a network.

   General infiltrations, packet sniffers or beacons, are not coded in this dataset, as most of the time no act of cyber malice is committed. They are monitoring techniques that search for certain information. If a potential incident is labeled as a packet sniffer or beacon, do not code it.

   When an infiltration is found, please try to delineate the type and decimal the number with the 4 (.1 logic bombs, .2 virus, .3 worm, .4 keystroke logging)

## II. Target type

1. Private/non-state (financial sector, power grid, defense contractor, media organization, MNC)
2. Government non-military (US State Department, government websites, government member website)
3. Government military (US Defense Department, US Cyber Command, US Strategic Command)

## III. Coercive objectives for initiators

1. Disruption: take down websites, disrupt online activities, usually low cost, low pain incidents such as vandalism or DDoS techniques

2. Short-term espionage: gains access that enables a state to leverage critical information for an immediate advantage example; an being Russian theft of DNC emails and publicly releasing them in a disinformation campaign.
3. Long-term espionage: seeks to manipulate the decision-calculus of the opposition far into the future through leveraging information gathered during cyber operations to enhance credibility and capability, an example being China's theft of Lockheed Martin's F-35 plans
4. Degrade: attempt physical degradation of a targets' capabilities, Example: USA's Stuxnet against Iran; create chaos in a country to invoke a foreign policy response

## IV. Cyber-enabled information operation (CIO) presence (1) or absence (0)

The term "information warfare" has become rather broad and meaningless, much like the term cyberwar. It can mean anything from attacks on information, simply stealing information, to managing the reception of information by calling into question the veracity of truth claims. For our purposes, we want to distinguish information warfare operations from the more universal awareness of what an attack on information is conceived as by the general public. We also want to avoid the broad definition of information operations as defined by the U.S. military, which includes electronic warfare, psychological operations, and social network exploitation, among others. To avoid muddying the waters more, we instead focus on information operations in the midst of cyber incidents/campaigns; what we call cyber-enabled information operations (CIO).

This restriction to operations launched during ongoing cyber operations allows us to focus on how information and data is weaponized adjunct to cyber incidents and campaigns. Rather than documenting more broad attacks on truth and meaning, we seek to understand how data can be manipulated and/or used to message in a coercive operation against a rival state.

The Head of Cyber Command, General Paul Nakasone distinguishes between espionage, disruptive and destructive forms of cyber conflict (Nakasone 2019: 12). We have covered similar forms in our coding of cyber events with a typology of disruptive, espionage, and degrading attacks (destructive is too limiting since destruction is so rare in cyberspace) in order to delineate different types of cyber conflict and their probability of achieve coercive effect (Valeriano, Jensen, and Maness 2018). We have found that the majority of attacks are espionage while degrading attacks are rare but also the most likely form to be coercive in terms of changing a target's behavior.

It is important to note the evolution of cyber conflict and the utility of operations in the information space as they are aided by these information operations. Nakasone offers a new form, noting "now we're seeing what many call a corrosive threat, which is the ability to weaponize information in order to conduct influence campaigns, steal intellectual property, or leverage someone's personally identifiable information" (Nakasone 2019: 12). We focus here on influence campaigns (messaging) and leveraging information (manipulation).

Noting a need to consider the evolving methods of conflict in cyberspace, we now code cyber-enabled information operations (CIO) as concentrated state level efforts to manipulate data for coercive purposes or those operations seeking to utilize compromised information to send specific messages to the adversary. The focus is really on the manipulation and messaging aspects of information operations.

A more encompassing definition seeking to count all instances where information was simply compromised or stolen would be needlessly broad and not helpful in understanding the coercive potential of information operations. Information operations do not merely steal data but seek to disseminate information when it might harm the adversary or alter that data to manipulate the sentiment in the opposition. Stealing information is espionage, a factor for which we already code with our coercive objective variable. To truly understand the coercive potential of information operations, we need to be more specific.

Cyber-enabled information operations (CIO) are therefore defined, for the purposes of these data, state-based actions, in the context of an ongoing cyber action, seeking to communicate a message or manipulate the reception of digital information for malicious purposes among a targeted population. The actions are intended to sow discontent, change policy direction, or serve as a warning to an adversary in the digital space.

**V. Did the objective achieve its goal?** Did the cyber incident achieve its intended purpose? For example, did the disruptive attack successfully shut down a website via denial or service? Did an espionage technique breach the intended network and steal the information it sought to acquire? Did the degradation achieve damaging its intended target?

**VI. Did the incident evoke a concessionary behavioral change?**
Did the objective of the initiator evoke a concessionary behavioral change? i.e., did the target state concede in some way to the initiator as a result of the cyber incident? Where processes or procedures changed? Did the direction of the state's foreign policy change?

**VII. Severity scale**

**10. Massive death as a direct result of cyber incident**
*Example* - NORAD hacked and missiles launched, Air traffic control systems manipulated, commercial airliner hacked and brought down
*Notes* - For this measure to be coded, a state must direct a cyber incident against another state's or private organizations' network where the system is manipulated, and massive loss of life is a result (over 100 deaths).

**9. Critical national infrastructure destruction as a result of cyber incident**
*Example* - power grid hack, hydroelectric dams shut down, indirect death
*Notes* - For this measure to be coded, a state's critical infrastructure must be breached and the network manipulated so that widespread functionality is disrupted for a significant period of time. These efforts have to be massive, impactful, and clearly intentional.

**8. Critical national economic disruption as a result of cyber incident**
*Example* - stock market price manipulation, critical e-commerce shut down for extended periods
*Notes* - For this measure to be coded, a sophisticated infiltration must be responsible for the manipulation of prices that affect stock market indexes and prices for extended periods of time. Another example would be a cyber incident being responsible for the slowing or shutting down commerce online. This attack must be severe and critically threatening beyond compromising payment systems.

**7. Minimal death as direct result of cyber incident**
*Example* - Auto hacked, pacemaker hacked

*Notes* - Here a state-sponsored cyber incident would be responsible for the death of an individual or group of individuals of another state by either hacking into the automobile of the victim(s) or causing it to crash, or if the victims(s) are dependent on a pacemaker to live and this device is hacked, leading to that person’s death.

**6. Single/multiple critical network infiltration and widespread destruction**
*Example* - (Stuxnet, Shamoon, Left of Launch)
*Notes* - For this measure to be coded, a single or multiple network that is critical to national security must be breached and widespread destruction must be successful. Critical stored information is destroyed or unrecoverable or functionality of the network must be limited to non-existent for a period of time.

**5. Single/multiple critical network infiltration and physical attempted destruction**
*Example* - (Flame, DoD secure network intrusion)
*Notes* - This measure entails the successful breach of a network(s) where damage is done, however the breached network is left intact in terms of functionality and recoverable losses.

**4. Widespread government, economic, military, or critical private sector network intrusion, multiple networks**
*Example* - (US OPM hack, DoD employee records stolen, IRS hack)
*Notes* –Phishing and intrusion espionage campaigns that successfully steal large troves of critical information, such as the OPM hack.

**3. Stealing targeted critical information from one network**
*Example* - (Chinese targeted espionage, government-sanctioned cybercrime, Sony Hack)
*Notes* - This involves the use of intruding upon a secure network and stealing sensitive or secret information. The theft of Lockheed Martin’s F-35 jet plans or the U.S. Department of Defense’s strategy in the Far East are examples. Or if the target was critical to national security or the objective of the attack had national security implications. The piggy-back method is another example of this severity type.

**2. Harassment, propaganda, denial and disruption**
*Example* - (Propagandist messages in Ukraine, Vandalism, DDoS in Georgia, Bronze Soldier dispute)
*Notes*–Mainly vandalism or DDoS campaigns, this measure is coded when pockets of government or private networks are disrupted for periods of time and normal day to day online life is difficult, but recoverable.

**1. Probing/packet sniffing without kinetic cyber**
*Example* - (Probing networks, packet sniffing)
*Notes* - Using cyber methods to breach networks but not utilize any malicious actions beyond that. Hacking a power grid but not shutting it down, planting surveillance technology within networks, and unsophisticated probing methods are examples of this severity level.

**0. No cyber activity**

## VIII. Damage type (conceptualized from Rid and Buchanan 2014)

1. Direct and immediate: The term direct in this context means that the damage done by the cyber incident was what was intended by the initiator and the costs of the cyber incident are felt immediately. The Russian DDoS attacks on Estonia's government and private networks in 2007 is an example, as the effective shutdowns cost millions of dollars in lost revenue for the Baltic country.

2. Direct and delayed. Stuxnet was intended to disrupt Iran's nuclear program by damaging the centrifuges at the Natanz plant, and it succeeded. The impact of this attack took a number of months if not years to slowly disrupt and damage these centrifuges through code manipulation.

3. Indirect and immediate. Indirect in this context means that the damage done by the cyber incident was not the original intent of the initiator. The stealing of confidential information from a bank or a breach in the Wall Street system is an example of this. The costs of these incidents are felt immediately. Reputational damage or loss of confidentiality is what to look for when coding this damage.

4. Indirect and delayed. If intellectual property is stolen by an initiator and it becomes publicly available, this may result in improved competition for states or private companies that did not have this technology or advantage prior. China stole the American company's F-35 jet plans, and if it gave these plans to Russia, the effects of this cyber incident would be indirect, and the costs would be felt at a future point in time.

## IX. Critical infrastructure

This nominal variable ranges from 1-17 and is coded as follows (see https://www.cisa.gov/critical infrastructure-sectors)**:**

1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Systems Sector
16. Water and Wastewater Systems Sector
17. Other (Election Infrastructure, Academia)

### X. Supply chain

The rise in the exploitation of data, software, hardware, and digital components, coupled with the reality of global supply chains and supply side trusted contacts, is a growing problem. One example is when an actor compromises a software company by inserting malicious code into their product used by a secondary target such as the SolarWinds incident. The supply chain is compromised because the software offered is providing a backdoor to a target. For this variable, we capture the presence or absence of a supply chain breach in binary form (“1” for supply chain breach, “0” otherwise).

### XI. Ransomware

Ransomware is also a cyber security issue that is growing in volume and severity. Once thought to be excusive launched from non-state actor criminal groups, certain states have recently been found initiating these acts. Ransomware is when an actor locks a target network out of its data access via cryptographic means, and then demands a ransom payment for this data access to be restored. Russia’s launch of Petya and then NotPetya in 2016-2017 had been targeting Ukrainian government and infrastructure networks, but these actions ended up spreading globally. North Korea has also been attributed to the WannaCry ransomware attack, which was also global and caused nearly $4 billion in revenue loss in 2017. The ransomware variable is coded as “1” if there is a presence of the act, “0” otherwise.

### XII. Specific political objective

Here we decipher as to why the cyber incident was launched in the first place. For example, for the Sony Hack the objective was to stop the release of the movie *The Interview*. A maximum of two political objectives are allowed.

### XIII. Sources cited

Here we provide the links to the sources which have indicated state responsibility for each incident in the dataset.

### Reliability Checks

For version 2.0 of the data, rigorous reliability checks were undertaken to investigate the reliability of our coding by our intern coders, as well as deciding whether the incident should be included in this version given the evidence of state responsibility. Project leaders assembled and went through the raw data of all incidents coded by the interns hired for this project. We held multiple sessions where coding was done independently, and then majority opinion decided on the variables’ values. Intercoder reliability tests were then estimated to establish the success of our efforts in ensuring trust and verification of the coding effort. Fleiss’ Kappa tests are appropriate for intercoder reliability when there are three or more coders. This score can be interpreted as finding to what extent the observed amount of agreement among raters exceeds what would be expected if all raters made their ratings completely randomly. For DCID 2.0, we obtained a Fleiss-Kappa score of .712, which denotes substantial agreement.

Furthermore, experts from the Professional Military Education (both students and instructors) system were recruited to help with the subjective coding of two key variables of interest. Objective achievement and concessions could vary by the individual since there is no objective measurement of such issues getting reliable variable coding is paramount. For the objective achievement dependent variable, we obtained a Fleiss' Kappa score of .496. The score of .646 denotes substantial agreement, which is to be expected as there were 15 different examiners involved in this effort. For the concessionary behavioral change dependent variable, we obtained a .589 Fleiss' Kappa score using the same number of coders, which is also within the substantial threshold. For the independent variables of compellence type, three authors code these variables and then came to agreement on the final values, obtaining a substantial agreement with Fleiss' Kappa score of .759.

**Variables for the Dyadic Cyber Incident and Campaigns (DCID) Dataset, Version 2.1 Campaign Sheet (Forthcoming)**

A. Cyber incident number (decided by dyad pair number and then earliest start date)
B. Dyad pair (combined COW country codes)
C. State A (first state in the dyad by lowest COW country code)
D. State B (second state in the dyad by higher COW country code)
E. Name of cyber incident
F. Incident Start Date (either specific date if available, accurate to the month otherwise)
G. Incident End Date (either specific date if available, accurate to the month otherwise, end date usually is when an incident is made public or eradicated by the target, or both)
H. Method of interaction/incident, 1-4 with decimal denotations for infiltrations (methods are listed below) for incidents:

1. defacements are vandalism;
2. DDoS, zombies, botnets, and the like will be denial of service;
3. any incident that uses spear phishing will be an intrusion, which includes Trojans, trapdoors, spear-phishing techniques, and backdoors. Intrusions are used in most theft/espionage operations;
4. infiltrations, are malware with specific and targeted payloads
    - .1 Logic bombs, wiper malware
    - .2 Viruses
    - .3 Worms
    - .4 keystroke logging

I. The type of target

1. private/non-state,
2. government non-military,
3. government military

J. The initiator of the interaction (COW country code)
K. The specific coercive strategy of the cyber incident

1. disruption,
2. short-term espionage
3. long-term espionage
4. degradation

L. Whether or not an information operation was utilized as a result of the cyber incident

0. absent
1. present

M. Whether or not the incident successfully achieved its objective; did it breach the target's network and fulfill its intended purpose

0. no
1. yes

N. Whether or not the political objective evoked a concessionary change in behavior of the target state.

0. no
1. yes

O. Damage type

1. Direct and immediate,
2. Direct and delayed,
3. Indirect and immediate,
4. Indirect and delayed

P. Deny/Reject (diplomatic negative foreign policy action, CAMEO score -4)
Q. Threat/Demand (diplomatic negative foreign policy action, CAMEO score -5)
R. Diplomatic negative combined CAMEO score
S. Negotiate (diplomatic positive foreign policy action, CAMEO score +7)
T. Agreement (diplomatic positive foreign policy action, CAMEO score +8)
U. Diplomatic positive combined CAMEO score
V. Economic reduce trade (economic negative foreign policy action, CAMEO score -5.6)
W. Economic threat (economic negative foreign policy action, CAMEO score -5.8)
X. Economic impose embargo, boycott, or sanctions (economic negative foreign policy action, CAMEO score -8)
Y. Economic negative combined CAMEO score
Z. Cooperate economically (economic positive foreign policy action, CAMEO score +6.4)
AA. Economic ease economic sanctions, boycott, embargo (economic positive foreign policy action, CAMEO score +7)
AB. Economic aid (economic positive foreign policy action, CAMEO score +7.4)
AC. Economic positive combined CAMEO score
AD. Military threat (military negative foreign policy action, CAMEO score -7)
AE. Military display of force (military negative foreign policy action, CAMEO score -7.2)
AF. Military use of force (military negative foreign policy action, CAMEO score -10)
AG. Military negative combined CAMEO score
AH. Military promise, intent to cooperate militarily (military positive foreign policy action, CAMEO score +5.2)
AI. Military cooperation (military positive foreign policy score, CAMEO score +7.4)
AJ. Military confidence building, aid (military positive foreign policy action, CAMEO score +8.3)
AK. Military positive combined CAMEO score
AL. Conventional foreign policy actions combined CAMEO score (campaign severity score)
AM. Cyber incident severity score, from incidents datasheet: converted to negative scores from positive in order to correspond with the conventional CAMEO scores
AN. Stated or interpreted strategic/political objective of the cyber incident

**What is searched for and recorded: Cyber Campaigns Sheet**

For cyber campaigns, we assume that cyber incidents launched by one rival state against another do not happen in isolation, and that conventional foreign policy actions during a certain time frame happen between states in conjunction or in coordination with malicious cyber operations. Examining the combined context of cyber conflict is an important consideration often left out of the conversation regarding the utility of cyber methods. While cyberspace can be considered its own domain, and the language we use often invokes this framework, the reality is that it is more of a layer (Choucri 2011) that interacts with other diplomatic, economic, and military tools at the same time, often in the same place. Cyberspace includes the digital form of software and human capital needed to launch destructive cyber acts, but it also includes the physical hardware that is located within states and territories. The targets that are of interest to cyber hackers are located somewhere. Invoking the physicality of the internet in many ways pushes us to think about the interactive context of cyber actions.

With the physical targets that are the goals of cyber operations, along with the personalities targeted for influence, we must consider the additive and combined context of cyber actions. There is a location, history, and personality inherent in all cyber actions that seek strategic intent. To properly understand how cyber strategies of rival states work, we must understand the context of these interactions, including the positive and negative steps states take to achieve effects.

Distinguishing between the carrot and the stick has been a traditional conceptualization of punishment and reward in international relations. The conceptual origins are from a cart horse conjecture, choosing between the reward (carrot) or running from punish (the stick). In coercion, it is important to remember that not all actions are punishments. Positive inducements can be more useful than punishment (Baldwin 1985), depending on the actor and their reward structures.

In our conceptualization of combined coercive actions, we account for positive inducements in the diplomatic, economic, or military categories. Diplomatic overtures, negotiations, and agreements are seen as positive steps forward where dialogue and a frank exchange of ideas takes precedent over threats. In economic maneuvers, negative sanctions are popular but so are positive events like freeing up previously seized money, removing sanctions, or exchange of cash and goods to remove ill will. Military actions include aid and cooperation in a positive sense to displays of force and engagement on the negative side of the spectrum.

An important caveat to these predictions is that it is not assumed that the initiating state coordinates these combined strategies on all fronts. While this might be true in the United States, in some states like Russia and China there is a lack of coordination between civilian militias, private hackers, and cyber criminals who might all be acting under the nationalist impulse, without direction. Assuming that states can coordinate cyber programs, often Special Access Programs (SAPs) that are often initiated in secret with other instruments such as diplomatic overtures from the State Department or military maneuvers from the Department of Defense, is impossible. However, it is not logically inconsistent to assume that regardless of the initiator's presumed lack of coordination, the target sees the instruments of power as coordinated if initiated within a certain time period. Although it has been often noted that attribution of cyber incidents is difficult to ascertain in real time, when under attack target states will have assumptions as to who the perpetrator is. With these assumptions underway, and the fact that the suspect is also initiating diplomatic, economic, or military action simultaneously, the target will perceive this as a coordinated attack and any combined coercive effect that is evoked from these actions will be present in the combined datasheet.

The coding of the conventional variables is timed to be within a reasonable window of the impactful cyber action that allows for a cyber campaign to fulfill its malicious intent as well as evoke a behavioral change in the target state. We therefore use logical cutpoints that attempt to capture how states initiate complex foreign policy actions against adversaries, and code any conventional foreign policy operation within one month of the start date of the cyber incident, which includes conventional action one month before and one month after the start date of the cyber incident. State decision-making and the subsequent implementation process of these complex and coordinated events take time, and a month before and after these cyber incidents allows for both enough time for these states to launch these combined strategies as well as logical cutoffs for our own coding efforts. When it comes to cyber events that are coded as espionage, we use a slightly different approach. Instead of coding conventional foreign policy action to coincide with the start date of the cyber interaction, which is suitable for real-time attacks such as defacements, DDoS, or sabotage attacks, for espionage events we use the one-month window for the end date of the cyber operation, which is usually when the exploitation becomes public and the target actor then reacts in a public setting to these actions, and the conventional foreign policy actions by the initiator during this time period will be assumed to be a combined assault in the eyes of the target when the event has become public.

For the collection of the conventional foreign policy data, the primary source of the events collection effort was derived from the Integrated Crisis Early Warning System (ICEWS) dataset, which consists of events data that spans the years 1995-present and includes events ranging from diplomatic meetings to military action and includes initiations and targets from both state and non-state actors (Boschee et. al., 2015). Variables are coded as either negative or positive based on whether they are a positive inducing foreign policy action or a negative, more threatening one. Coded variables in this dataset can include diplomatic negotiations, which include high level meetings between state diplomats as well as telephone conversations between leaders, economic reduction of trade, where bilateral deals are altered or terminated, and military usage, which includes all use of conventional military force by one state against another. This variety as well as differing severity of foreign policy actions make the use of ICEWS data the most-suited and encompassing collection of non-cyber variables for the purposes of this analysis.

## XI. ICEWS diplomatic conventional foreign policy actions

Only four specific variables recording diplomatic foreign policy action are recorded in the cyber campaigns sheet for this study. We code only diplomatic action that has the potential to change the decision-making calculus of the target state in some way. Therefore, only diplomatic action that are either labeled as deny/reject (CAMEO score -4), demand/threat (CAMEO score -5), negotiate (CAMEO score +7), or agreement (CAMEO score +8) are recorded and included with the corresponding cyber incident if it is present in the assigned time period discussed above. Other diplomatic variables are excluded as they are very benign, with CAMEO scores close to zero, and also very ubiquitous in the ICEWS dataset, as most countries will be in contact in some way numerous times on a daily basis, where decision-making calculus is rarely changed as a result of these exchanges. We are looking for diplomatic variables that have the ability to be coercive, deceptive, or appeasing, and the variables included the diplomatic category capture this potential, especially when combined with other instruments of power.

## XII. ICEWS economic conventional foreign policy actions

On the negative (conflictual) side, we record the presence or absence of three variables: economic reduction in trade (CAMEO score -5.6), economic threats (CAMEO score -5.8) and economic imposition of sanctions, boycotts, or embargos (CAMEO score -8). For positive (cooperative) economic scores included in the campaign datasheet, there are also three variables that are recorded: economic cooperation (CAMEO score +6.4), economic ease of sanctions, boycotts, or embargos (CAMEO score +7), and economic aid (CAMEO score +7.4).

## XIII. ICEWS military conventional foreign policy actions

There are also three variables each for the negative and positive sides of military action by states. On the negative side, this includes military threats (CAMEO score -7), military displays of force (CAMEO score -7.2), and military use (CAMEO score -10). For positive military cooperation scores, we include the following: military promise to cooperate (CAMEO score +5.2), military cooperation (CAMEO score +7.4), and military confidence building/aid (CAMEO score +8.3).

## XIV. Combined conventional foreign policy CAMEO scores: Cyber Campaign severity scores

For this score, we simply add up the comprehensive all of the conventional foreign policy actions and their corresponding CAMEO scores to give us a raw campaign severity score, which is separate from the cyber incident severity score. If there is nothing except conflictual (negative CAMEO scores) variables, then the severity score for that cyber campaign will be more negative. For events that have a mix of negative and positive (cooperative) variables, the conventional scores should be closer to zero. For positive inducement-heavy campaigns, the scores will be above zero. These scores will then be able to be juxtaposed against the assigned cyber incident severity scores in order to unveil the most cantankerous as well as the most restrained dyadic relationships for states who have decided to engage in international cyber conflict.

## XV. Cyber severity scores, convert to negative scores from positive, where 1 is less severe and 10 is the most severe (see incident coding procedures for severity).

## References:

Baldwin, David A., 1985. *Economic Statecraft*. (Princeton University Press).

Boschee, Elizabeth, Jennifer Lautenschlager, Sean O'Brien, Steve Shellman, James Starz, Michael Ward. 2015. "ICEWS Coded Event Data, doi:10.7910/DVN/28075 **.** Harvard Dataverse, Volume 15.

Choucri, N., 2012. *Cyberpolitics in International Relations*. (Cambridge: MIT Press).

DHS CISA., 2021. "Critical Infrastructure Sectors" available at: https://www.cisa.gov/critical-infrastructure-sectors

Goldstein, Joshua S., 1992. A conflict-cooperation scale for WEIS events data. *Journal of Conflict Resolution*, 36 (2): 369-385.

Goodman, Will. 2010. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* Fall 2010: 102-135.

Jones, Daniel M., Stuart A. Bremer, and J. David Singer. 1996. "Militarized Interstate Disputes, 1816-1992: Rationale, Coding Rules, and Empirical Patterns." *Conflict Management and Peace Science*, 15 (2): 163-215.

Klein, James P., Gary Goertz, and Paul F, Diehl (2006) The new rivalry dataset: procedures and patterns. Journal of Peace Research 43 (3): 331-348.

Maness, Ryan C., Brandon Valeriano, and Benjamin Jensen. 2017. *The Dyadic Cyber Incident and Dispute Dataset, version 1.1*, available at: https://drryanmaness.wixsite.com/cyberconflcit/cyber-conflict-dataset

Nakasone, Paul M. 2019. "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1): 10-15.

Rid, Thomas and Ben Buchanan 2014. "Attributing Cyber Attacks. *Journal of Strategic Studies*, DOI: 10.1080/01402390.2014.977382.

Schrodt, Philip. 2012. "CAMEO: Conflict Mediation Event Observations Event and Actor Codebook." http://data.gdeltproject.org/documentation/CAMEO.Manual.1.1b3.pdf

Thompson, William R. 2001. Identifying rivals and rivalries in world politics. International Studies Quarterly 45 (4): 557-86.

Valeriano, Brandon and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011." *Journal of Peace Research*, 51 (3): 347-360.

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press).

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness 2018. *Cyber Strategy: The Changing Character of Cyber Power and Coercion*, (New York: Oxford University Press).