Codebook for the Dyadic Cyber Incident and Dispute Dataset Version 1.1
Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen
August 1, 2017

Overview

This codebook presents a point of reference for variables for dyadic rival states that are in Dyadic Cyber Incident Dataset (DCID) v 1.1 for the years 2000-2014. This builds on the previous version 1.0 released by Valeriano and Maness (2014, 2015). 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, then called the Cyber Incident and Dispute dataset (CID). Here we are focused on observable incidents between international nation-states since interactions between criminal elements and other non-state actors would require different data collection strategies and theories. Version 2.0 of our data will expand the data collection to all states and non-state actors.

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 disputes. 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. For a series of cyber incidents between two states over a limited period of time, we use the term 'cyber disputes.' This appendix pertains to research involving only incidents and the description of coding efforts for these individual events will only be discussed.

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 dispute was 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. 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. (The 2015 modification in the OUP book contained 111 incidents among 45 disputes, where an espionage dispute between China and India was added). Version 1.1 has 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.

Specific Procedures

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

An example of a Correlates of War dataset is 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. 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. Therefore, 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 events data searches will be undertaken but for now we are confident we can maintain an active dataset using focused search methods.

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 eg. Iran" AND "participant B eg. 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 12/31/2014.

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

What is searched for and recorded:

A. The dyad (states involved), only two states recorded per incident
B. Start and end date of interaction
C. 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 usually worms or viruses, but can also be logic bombs and keystroke loggings.
D. Type of interaction (nuisance, defensive, offensive)
E. The type of target (private/non-state, government non-military, government military)
F. The initiator of the interaction
H. The specific coercive strategy of the cyber incident (disruption, short or long-term espionage, degradation)
I. Whether or not the incident successfully achieved its objective; did it breach the target's network and fulfill its intended purpose
J. Whether or not the political objective evoked a concessionary change in behavior of the target state.
K. 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.
L. Whether or not a third party was a target of the interaction 1= yes, 0 = no: This is more commonplace, especially for espionage campaigns (intrusions)
M. Whether or not an official government statement was issued by the initiator, 0= no comment, 1= denial, 2= acceptance, 3-multiple; this will help in the responsibility coding; although most of the time governments will deny or not comment about their part in cyber incident initiation.
N. Severity level on the 0-10 scale level, given below for both incidents and disputes
O. Damage type (1. Direct and immediate, 2. Direct and delayed, 3. Indirect and immediate, 4. Indirect and delayed)
P. A key source for the cyber incident
Q. Any special notes pertaining to the 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, 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 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: 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. Denial of Service: DDoS, 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. Intrusion: "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. Infiltration: 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 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. Interaction type

1. Nuisance (probing, disruption, chaos); most vandalism and denial of service incidents, intent is disrupting the day to day operations of a network, easily removable by target
2. Defensive operation (Cisco Raider, Buckshot Yankee, Israeli operations against cyber-jihad); the initiator must be the victim of a cyber incident first; these are defensive measures launched by a target where it becomes the initiator
3. Offensive strike (GhostNet, ShadyRAT, Stuxnet); intent is usually theft or espionage or to disrupt a specific national security strategy of a target, most intrusions and infiltrations.

III. 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)

IV. 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 critical network widespread destruction

Example - (Shamoon, DoD taken offline, Lockheed Martin database wiped out)

Notes - For this measure to be coded, a single 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 critical network and physical attempted destruction

Example - (Stuxnet, Flame, DoD secure network intrusion)

Notes - This measure entails the successful breach of a network 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 theft of information

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

Example - (Chinese targeted espionage, government-sanctioned cyber crime, 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. The United States' NSA was able to piggy back on China's Byzantine Series undetected and spy on the targets that the original espionage was spying upon.

2-Harrassment, propaganda, nuisance 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 without kinetic cyber

Example - (US NSA dormant infiltrations)

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

V. 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.

VI. 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

VII. 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.

VIII. 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?

IX. 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?

Reliability Checks

For version 1.1 of the data, rigorous reliability checks were undertaken to investigate the reliability of our coding of the compellence variables. Experts from the Professional Military Education (both students and instructors) system were recruited to help with the subjective coding of the 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. 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. For the objective achievement dependent variable, we obtained a Fleiss' Kappa score of .496. Fleiss' Kappa test 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. 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 amount of coders, which is also within the substantial threshold. For the independent variables of compellence type, the three authors code these variables and then came to agreement on the final values, obtaining a substantial agreement with Fleiss' Kappa score of .759.

X. Variables for the Dyadic Cyber Incident and Dispute (DCID) Dataset, Version 1.5

Variable Number	Variable Name	Variable Description
1	Cyberincidentnum	Cyber incident number
2	DyadPair	State Pair ID (COW codes)
3	StateA	First state in dyad
4	StateB	Second state in dyad
5	Name	Name of cyber incident:
6	interactionstartdate	Cyber incident start date
7	Interactionenddate	Cyber incident end date
8	Interactiontype	Type of cyber interaction for incidents 1- Nuisance 2- Defensive operation 3- Offensive strike
9	Method	Cyber method utilized 1- Vandalism 2- Denial of Service (DDoS) 3- Intrusion 4- Infiltration 4.1 - Logic bomb 4.2 - Virus 4.3 - Worm 4.4 – Keystroke logging 5- Vandalism and Denial of Service (disputes only) 6- Intrusion and Infiltration (disputes only)
10	APT	Advanced Persistent Threat? 1- Yes, 0- No
11	Targettype	Type of target by cyber incident or dispute 1- Private/non-state 2- Government non-military 3- Government military
12	Initiator	State that initiated the incident or dispute (COW code)
13	Coercive objective	Objective of the initiating state (disputes only) 1- Disruption 2- Short-Term Espionage 3- Long-Term Espionage 4- Degrade
14	Political objective	Statement of political objective of initiator
15	Objective success	Did the objective succeed? 1-Yes, 0-No

16	Concession	Did the target concede? 1- Yes, 0- No
17	3rdpartyinitiator	Third party involved with initiating state? 1- Yes, 0- No
18	3rdparty target	Third party involved as a target? 1- Yes, 0- No
19	Govtstatement	Statement from the initiating state? 0- No comment, 1- Denial, 2- Acceptance, 3- Multiple statements
20	Severity	Severity level of incident or dispute (for disputes code the highest incident severity 1- Probing without kinetic cyber 2- Harassment, propaganda, nuisance disruption 3- Stealing targeted critical information 4- Widespread government, economic, military or critical private sector theft of information 5- Single critical network and physical attempted destruction 6- Single critical network widespread destruction 7- Minimal death as a direct result of cyber incident 8- Critical national economic disruption as a result of cyber incident 9- Critical national infrastructure destruction as a result of cyber incident 10- Massive death as a direct result of cyber incident
21	Damage type	1. Direct and immediate 2. Direct and delayed 3. Indirect and immediate 4. Indirect and delayed
22	Source	The news source for the cyber interaction
23	Notes	Any special notes pertaining to the interaction

References:

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.

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

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).