Journal of Strategic Security

Volume 16 | Number 1 Article 5

Cyber Cases: The PICCA Framework for Documenting Geopolitically Relevant Cyber Action

Chris Bronk
University of Houston, rcbronk@gmail.com

Nathan Jones
Sam Houston State University, nxj008@shsu.edu

Recommended Citation
Bronk, Chris and Jones, Nathan. "Cyber Cases: The PICCA Framework for Documenting Geopolitically Relevant Cyber Action." *Journal of Strategic Security* 16, no. 1 (2023) : 72-89.
DOI: https://doi.org/10.5038/1944-0472.16.1.2068
Available at: https://digitalcommons.usf.edu/jss/vol16/iss1/5

Cyber Cases: The PICCA Framework for Documenting Geopolitically Relevant Cyber Action

Abstract

This article presents a novel framework called the Policy Informative Cyber Case Analysis for cyberattack incidents. The aim of this framework is to provide a structured documentation and translational assessment tool for cyber incidents of geopolitical significance to a broader policy audience. The article discusses case study method as applied to cyber incidents, situates the framework amongst other useful methods, discusses the application of structured analytic techniques (SAT) such as "chronologies and timelines" and "devil's advocacy," presents the framework, and provides conclusions. Cyber incident cases, primarily the 2015 attack on the Ukrainian electric-grid is used throughout to elucidate the utility and application of the framework.

Introduction

In the space of about two decades, cybersecurity has grown from relative curiosity to great significance in international security. Once considered, “weapons of mass annoyance,” the instruments of cyber action are now considered more than mere nuisance.[1] Whether for purposes of espionage, covert action, or criminal activity, cyber action has grown to occupy a prominent position in the security studies literature as well as national security discourse.[2] The number of research papers and articles on the topic has grown steadily in political science, international relations, and public policy.[3] Despite growth in interest, there are still issues in understanding how to form generalizations from observation.[4] Much of what is written on events of cyber conflict, frequently labeled cyberattacks, are the analyses of individual incidents. Often, they are highly technical in nature and not approachable to individuals without deep background in Information and Computing Technologies. These are usually a form of case study, and many are of high quality, but they raise questions as to what the parameters of such a study should be. Offered here is a consideration of the application of case study methods to cyberattacks of relevance to international security.

In asking what makes for a well-constructed, geopolitically-oriented case study regarding a cyberattack or campaign, we are less interested in the particulars of system compromise. This is something of great importance to the cybersecurity technical community. Of greater salience is the impact of a cyberattack. What a policy reader may take away from the details of an incident are far different than those of interest to a computer scientist. A case study may detail an incident such as action undertaken against the Iranian nuclear enrichment program or attempts to temporarily disable portions of the Ukrainian power grid. However, in these cases and others, there are potentially enormous wells of detail regarding the targets attacked, the methods of action, and geopolitical factors available for analysis.[5] Each cyberattack potentially involves a wealth of technical data regarding system compromise, manipulation, and subversion. These pieces of information may answer the What and how questions regarding a cyberattack.

Beyond the technical details exists a set of why questions that also belongs in analysis of cyberattacks and campaigns of attacks.[6] There is a motivation to employ cyberattacks, often in combination with other forms of covert action, diplomatic activity, or military force to achieve their political goals. For instance, the first major cyberattack against a North Atlantic Treaty Organization (NATO) member, Estonia, in 2007, aimed to degrade the function of that country's information infrastructure, which had been heavily computerized following its breakaway from the Soviet Union. Answering why Estonia became a target is straightforward.[7] Its government moved a Soviet memorial and in response a rhetorical storm emanated from Moscow coupled with cyber action. Ostensibly, although offended, Russia wasn't willing to invade or drop bombs on a NATO member, so it employed cyber methods instead.[8] The following year, when Georgia received Putin's wrath, cyber action was combined with military force.[9] Since the events of 2007-2008, many more state-launched or state-sponsored cyberattacks have occurred, and to understand their relevance to international security, should aim to develop our knowledge regarding how to assess and characterize them as issues of policy.

Offered here is consideration of cybersecurity case studies relevant to international security. The authors wish to nail down what is important to know and document from the inherently interdisciplinary information, from computer code to public statements by government officials, that makes up a cybersecurity case.[10] To do so, the authors provide an overview of case study methods, with emphasis on international security; review several significant case studies of geopolitically relevant cyberattacks; offer a framework, the Policy Informative Cyber Case Analysis (PICCA) for case analysis of such attacks; and provide observations from graduate student case study assignments undertaken in an interdisciplinary cybersecurity program. Our goal is to provide guidance for scholars in cybersecurity to employ in documenting the phenomena that encompass cyber actions, an area of tremendous growth in contemporary international security. Case studies are a frequently employed tool for explaining complex events or phenomena.[11] They have considerable explanatory power but are criticized for being flawed by author subjectivity or being atheoretical in nature. What does and does not belong in a case is an interesting problem. Thus, "there is a need for articles that provide a comprehensive overview of the case study process from the researcher's perspective, emphasizing methodological considerations."[12] These articles must address, "specific design requirements, data collection procedures, data analysis, and validity and reliability."[13] This thinking should extend to case studies in

DOI: https://doi.org/10.5038/1944-0472.16.1.2068

cybersecurity, in particular the forms of cyber action that are related to international security.

Guideposts and Parameters of Policy-Oriented Cyber Case Building

The PICCA case study method presented invites questions of how to format reporting of case analysis of cyberattack cases. First, the research framework and pedagogical assignment posited here, lays the foundation for in-depth single, small-N, and large-N case method studies across a variety of possible research projects. Second, this project established in-depth single case studies across multiple variables with an emphasis on time order. This allows for the analytical method of process-tracing wherein the "researcher examines histories, archival documents, interview transcripts…to see whether a causal process a theory hypothesizes or implies in a case is in fact evident in the sequence and values of the intervening variables of that case."[14] Researchers will likely also use this case study reservoir for heuristic case studies which "inductively identify new variables, hypotheses, causal mechanisms, and paths."[15] Because this framework is qualitative and allows for judgement and assessment, there is a high probability that new variables will be identified in the application of this framework.

Third, this framework establishes comparative cases studies through what George and Bennett would call the method of structured focused comparison. This seminal work argues that case studies must have structure to focus on the same key variables:

> The method is "structured" in that the researcher writes general questions that reflect the research objective and that these questions are asked of each case under study to guide and standardize the data collection, thereby making systematic comparison and cumulation of cases possible. The method is "focused" in that it only deals with certain aspects of the historical cases examined. The requirements for structure and focus apply to individual cases they may be later joined by additional cases.[16]

Fourth, the reservoir of cases built here eases the task of case selection for future research designs. Case selection is important in this qualitative, positivist work and researchers are admonished typically not to choose cases on variation in the dependent variable.[17] To ease this process, PICCA produces not just useful case studies for immediate analysis, but a reservoir of viable preliminary cases for researchers, intelligence analysts, or corporate security analysts. This reservoir gives them a sense of the universe of geopolitically significant cases collected within their organizations and allows them to select optimal cases appropriate to their research or policy objectives.

Because the system in which the data (cases) gathered here is systematic and collected like specific variables, the cases can serve as a preliminary case study reservoir for later more complex case study designs based on specific objectives. Additionally, more cases are incorporated as they become available as George and Bennett discuss.[18] The cases can also provide important process tracing within case analysis or in comparison case study designs.

The establishment of a baseline or working sense of the cases available and some general trends, even if initially anecdotal, or biased based upon opensource availability, is still highly useful. No data set is perfect, and the bias of that which is in the opensource or reported in the media, is common in many respected data sources. For example, the Armed Conflict Location Event Data Project (ACLED), geospatially catalogues and collects data on open-source political violence events in a systematic fashion, acknowledging that there may be missing events, but systematically trying to eliminate them.[19]

Structured Analytic Techniques (SAT)

The cases gathered here, also provide preliminary data, that can then be reorganized for analysis under what the intelligence community calls structured analytic techniques (SAT).[20] One such readily applied SAT these structured cases lend themselves to is “chronologies and timelines.”[21] Given this system emphasizes the timing of events, the underlying data thus lends itself to further deep chronological analysis including the creation of visualized horizontal or vertical linear timelines that can help, policymakers, juries, and research audiences rapidly understand the evolution of events related to the cyber incident. As Pherson and Heuer note, it is important not to assume causation solely because an event preceded an outcome. Further researchers must be imaginative in identifying relevant contextual events.[22]

Other structured analytic techniques are applicable to the cases gathered and structured within this framework. For example, the devil's advocacy technique is particularly relevant for aspects of attribution of cyber-attacks, which is notoriously difficult in the of cyber operations.[23] There may be assumptions that a specific malign actor(s) or advanced persistent threat(s) (APTs) are responsible for a particular attack. Related are the costs and consequences to a nation or corporate actor's credibility if it publicly gets analysis of an attack wrong.

This scenario is not hypothetical. As Beebe and Pherson document, a water plant in Curran-Gardner Illinois suffered a pump failure after it switched on and off repeatedly.[24] This occurred months after SCADA system access from an IP address in Russia. The Illinois State-Wide Terrorism and Intelligence Center issued a note that the event was an attack from a Russian IP address on a piece of US critical infrastructure. It was subsequently determined that the Russian IP access was from an authorized user accessing the system while on vacation in Russia and again on his flight layover in Germany. Thus, as Pherson and Beebe describe, to avoid such a scenario, institutions can take these cases through a devil's advocacy process in which a small analytical team attempts to tear apart the dominant narrative and present the best case against the existing framework by assessing its gaps and assumptions.[25]

Comparing to Other Useful Frameworks

There are many other useful cyber incident gathering systems and publicly accessible fora. MIT's Sloan School published a business case study that covers a cyberattack undertaken against a major financial institution.[26] Healey and Grindal offered a series of historical cases to describe the evolution of cyber action.[27] A mature effort in construction of homogenous, if technically-oriented cases is the MITRE ATT&CK™ framework.[28] This is a highly useful framework for IT professionals who need to protect information resources by immediately patching vulnerabilities or removing malevolent code. This system is useful for establishing the tactics, techniques, and procedures (TTPs) of cyber events which can help lend credence to assertions about attribution of potentially deniable attacks.[29]

This methodology differentiates itself from other useful cyber incident data gathering forums such as MITRE ATT&CK™ in a few ways. First, this methodology is more strategic and less tactical. Attention goes beyond specific code and computational assessment, with emphasis on the broader qualitative case study, its timing and chronology, and a qualitative assessment of its geopolitical significance. Second, the focus is on presenting the case study in a way that is digestible for non-technically oriented policymakers. In this fashion, this framework provides national and homeland security utility for policymakers. Third, the framework presented here assumes the addition of further cases and the application of further structured analytic techniques.

Parameters

Cyber incidents worthy of international security case analysis occur with increasing regularity. Knowing how to document cyber activity is valuable to many organizations, from corporations and governments to academics and security specialists. These actions continue to rapidly evolve in terms of complexity and sophistication. Cyberattacks are multi-parametric events broken down into taxonomic categories.[30] These categories involve a broad set of activities including targeting, preparation, compromise, infiltration, manipulation, and closure. Information regarding cyberattack may be heterogenous and varied but those actions typically violate the confidentiality, integrity, or availability of a computer system or systems.[31] The actions of unauthorized parties employing cyber means may be designed to produce criminal, intelligence, economic, or political outcomes. The actions of an actor wishing to subvert a system is an incident, not an attack, especially until more information is known about it.

The distinction between incidents and attacks is necessary, as the latter often includes educated guesses regarding attribution, the who done it of the matter.[32] In this framework for case analysis of cyber action, the incident is the core identifier. Targets, techniques, and vulnerabilities may reappear, but the combination of those attributes is what makes for a unique incident.

In documenting a cyber incident (which may or may not be an attack), there are two chief descriptors of incident identity. One is the system targeted. For instance, the cyberattack against the safety system of a petrochemical facility at Al Jubail, Saudi Arabia in 2017 is referred largely to by the type of system impacted, Schneider's Triconex.[33] see incidents identified either by the targeted location or the system subverted. Some examples of this include the attack on Ukraine's power grid or SolarWinds' software development environment. Another descriptor for cyberattacks is the malicious software employed in the attack. Although the reputed United States-Israeli cyberattack against Iran's nuclear enrichment activity was undertaken largely at Natanz, it was the name of the malware employed, Stuxnet, that came to be synonymous with the event. While the target of Stuxnet was unknown for some time, the cyberattack malware employed was not. Relatedly, the cybersecurity analytic community is constantly creating new codewords for malicious binaries and other technical aspects of cyberattacks. Multiple codewords may describe a single piece of malware. Just keeping those straight can be a challenge.

Part of the incident's uniqueness has to do with where and when it happened, as well as the processes through which the event occurred. It may not always be clear why a particular system is targeted, or if a system or organization was even intended to be a target.[34] Remember, opportunistic computer hacking has a large place in cybersecurity. But the hacks that are relevant to the public often are anything but opportunistic and specificly intended to produce a premeditated result. This is an applicable concept in major incidents, for instance the cyber action undertaken against Ukraine's electrical grid in 2015. A year after the annexation of territory in the Crimea, that cyberattack indicated that Russia was willing to apply cyber means to produce a kinetic event, the disruption, damage, and destruction of Ukraine's electrical grid.[35] Throughout the paper, the authors use this incident as a heuristic device for our framework and reference it as explain each component of the framework.

The example must have a name, and it is Ukrainian power grid kinetic cyberattack. Names for cases should clearly identify the incident while being easy for any reasonably well-educated reader to understand. The names of malicious software employed in this attack are important to the technical communities of cybersecurity but may be largely meaningless to a more policy-oriented audience. While major cases such as Stuxnet or Shamoon have broad meaning to technical cybersecurity experts, these are code-names applied to the computer software distributed to produce the result observed. The software code employed in a cyber incident is often its most important artifact, but that name does not necessarily mean much in isolation. Having the target in the name may be useful, but when the affected organizations are many and the impacts varied across them, a simple name based on target and outcome may fail to describe the phenomena at hand. The name for the attack against Ukraine offered here describes the target and the outcome, a kinetic cyberattack. A kinetic cyberattack is an incident in which the attacker subverts computers controlling machines producing a physical event, in this case disruption of the electrical delivery system, is manifested. The 2016 data destroying cyberattack launched against Ukraine that also impacted commercial entities Møller Maersk, Mondelez, and DHL is widely known as Petya/Not-Petya. That name reputedly is a reference to a satellite weapon featured in a 1995 James Bond film.

The creation of code-names in cybersecurity is complicated by the number of actors creating them. There is no international organization solely responsible for identifying these incidents but rather a miscellany of government agencies, cybersecurity service and tool vendors, and software firms discovering them and giving them names. While the Mitre Corporation has developed a system for identifying vulnerabilities in software and systems, it appears no single convention on naming cyber events. One person's Stuxnet is another's Olympic Games.[36]

Beyond naming there are other key items that belong up front in the PICCA format. Where the attack occurred is one. This is complicated by the distributed nature of information technology infrastructure, but targets of attacks are organizations that have physical as well as virtual homes. Returning to our Ukraine power grid case, can identify a location, the Ivano-Frankivsk region of the country. That is where the power companies affected by the attack are located. Remember, are not attempting to place any marker about attribution here. Stuxnet first impacted process control computers in Natanz, Iran and Shamoon deleted data on Saudi Aramco computers in Saudi Arabia and the company's other offices outside the kingdom.

Identifying when a cyberattack occurred can be thorny as well. In our Ukraine case, the physical manifestation of the attack occurred on December 23, 2015. know this because electricity customers in Ivano-Frankivsk reported service interruption for several hours. Local, national, and, eventually international, news sources covered the outage. Forensic data from the affected companies shared in the cybersecurity technical community indicated a pattern of probing and other malicious activity that stretched from 2014 to 2016 and likely beyond. This attack is related to other attacks on Ukraine that have stretched from the election of Ukrainian leaders unfriendly to Russia all the way to the war still ongoing between the two countries at the time of writing. In documenting cyberattacks, asking when is not necessarily ascertaining a fixed point but rather often identifying a timeline.

After identifying place and time, the logical next requisite piece of information is to know the impact of the cyberattack. Regarding the Ukrainian power grid kinetic attack, the most visible outcome was that the attack halted electricity distribution at three Ukrainian power companies (*oblenergos*) for several hours impacting 225,000 customers. Important to understanding individual incidents or attacks is background information about cyber activity. In this case, cyberattacks against Ukraine grew significantly in the wake of the 2014 Euromaidan revolution, in which a government aspiring to improve relations with Western European nations replaced one with a strong tilt toward Russia.

Eventually, the attack ends, which would summarize in our case template.

> According to DHS, three Ukrainian oblenergos experienced coordinated cyber attacks that were executed within 30 minutes of each other. The attack impacted 225,000 customers and required the oblenergos to move to manual operations in response to the attack. The oblenergos were able to restore service after an outage window lasting several hours.

The third leg upon which a policy-oriented case analysis of a cyberattack rests is in fleshing out the matter by which it is resolved. A key area of cybersecurity is that of incident response.[37] In this area, time matters greatly. When hospitals, power companies, or banks fall victim to disruptive or destructive attacks, a principal concern is in returning to normal. But for assessing relevance to national security or public policy, other issues matter as well. First is an assessment of damage and the question of whether that damage was intended or not. Also, critically important among our concerns is attribution of the attack's source, a particularly tricky area.[38] That said, attribution plays out at degrees of less than certain precision, often based on circumstances beyond the technical methodology. Choice of target is often an important clue.

Finding the Policy-Salient Features

Cyberattacks may be precisely targeted. The 2020 espionage cyberattack against computer network management software developer Solar Winds is such a case. The perpetrators gained access to the company, escalated their access privileges to its software development environment, and made changes to the software that rendered many of its customers vulnerable to compromise. There is a great degree of certainty that the Solar Winds development environment, ostensibly managed at the company's headquarters in Austin, Texas, was manipulated by malicious outsiders.[39] also have a good idea of when the compromise occurred and when it ended, after at least two security vendors found evidence of the hack on their own systems. The individuals who compromised Solar Winds network likely gained their initial foothold in September 2019 and likely retained access until security firm Mandiant revealed their knowledge of the incident in December 2020.[40]

Timing and location can also be especially interesting. On Friday, February 5, 2021, the water treatment plant for Tampa suburb Oldsmar, an outside party compromised Florida. Menacingly, the attacker took control of the plant's control system and issued instructions to increase the level of sodium hydroxide (lye) in the water being treated to potable levels to 100 times the normal amount.[41] This was a dramatic new development around industrial control systems (ICS) or operational technology (OT) security. Not only was the control system breached, but also manipulated by an unauthorized party to produce a potentially dangerous concentration of a chemical compound.[42] would consider Oldsmar an ICS or OT case exemplar, but there is another nuance to be teased from its location and time. The water plant serves a small suburb of Tampa, a metropolitan area of some four million. It was not the water plant at U.S.

DOI: https://doi.org/10.5038/1944-0472.16.1.2068

Central Command or Special Operations Command headquarters at nearby MacDill Air Force Base. But the timing was interesting. Oldsmar happened on the Friday before the Superbowl, held that weekend in Tampa. That timing could be completely unimportant or suggest possible adversary signaling.[43] Thus, must cast a wide net on time and place in trying to understand the nuances of cyber action.

In addressing the nuance of each cybersecurity case, analytic opinions matter. Creating an **assessment** may require reading malware source code, combing through multiple news stories, interviewing experts, and careful study of computing products, both hardware and software.[44] Cybersecurity assessments may cover a great many technical details.[45] In the case of major incidents, multiple cybersecurity firms may often publish findings based on the information their products and services produce. Cybersecurity is essentially a distributed analytic enterprise in which technologists and other experts from commercial entities, government, and academia often produce complementary or collaborative research. Much of the information found in a cybersecurity case is more quantitative or computational in nature, but there also may be elements present in a case that are more subjective. This subjectivity may extend to the volatility of an incident.[46] Incidents with grave implications for public health and well-being are of great concern, however espionage operations that may "prepare the battlefield" are of concern too. Another measure of significance may be the sophistication of an attack. Cyberattacks that exploit known vulnerabilities may be less noteworthy than those that employ previously unknown vulnerabilities for the first time.

Such subjectivity includes the why of the incident. Oftentimes, cyber incidents occur simply because an organization is unaware of an unknown vulnerability that is exploited by an outside actor with unclear or purely criminal intent. In other cases, the attacking party targets the organization for economic or political reasons, such as stealing information or knocking critical services offline. But asking why a cyberattack would occur, begins the process of attribution. By asking why something happened, it gets at offering analysis regarding the **intent** of the incident. Intent and **attribution** allow us to place a cyberattack in a framework. Here analysts may want to engage in a *cui bono* logic or ask the question who benefits from the attack? In doing so it is important to overtly state where the logic is used and the underlying assumptions in its use. Common are those involving espionage, the violation of confidentiality for intelligence purposes. Microsoft's revelation of a compromise of its Exchange email technology in 2021 immediately smacked of an espionage operation. By breaking Exchange, the perpetrators clearly wished to gain access to large quantities of corporate or government email.[47] This could be employed for all manner of economic and political purposes. Unsurprisingly, the United States, European Union, and NATO identified China's intelligence services as culpable for the attack.

Ultimately, there is an issue of boiling down a great deal of technical information for case analysis of cyberattacks. This raises important questions about where different kinds of information fit in a case.[48] Not every rumor, allegation, or technical specific matters to understanding an attack, however each attack usually adheres to an anatomy of sorts that may be approachable to a policy, rather than purely technical, audience. This is the focus of our next section.

A Policy Centric Case Process

Moving beyond the geographic and temporal location of cyber incidents as well as rough estimates of impact, it makes sense to identify information that found on three stages of cyberattack:

1. Reconnaissance and preparation;
2. Execution; and
3. Mitigation and resolution.

Each of these phases is important in understanding the dynamics of a hostile act undertaken through cyberspace.[49]

Reconnaissance and preparation encompass the process of identifying and preparing a target. The execution of the attack is typically the headline-generating event, such as the theft of data or disruption of systems' operation. At the mitigation and resolution phase, the emphasis for systems' operators is in restoring service while for other parties, attribution of the attacker or detection of previously unknown vulnerabilities may be of greatest interest. While opinion may differ on how to unpack the component parts of a cyber incident, these three encompass most of the pieces of one.[50]

https://digitalcommons.usf.edu/jss/vol16/iss1/5
DOI: https://doi.org/10.5038/1944-0472.16.1.2068

Some cyberattacks are well-prepared, targeted, and intentional. Others are based on opportunity, or even worse, collateral damage of a broad attack. These outcomes are largely the basis of the reconnaissance and preparation phase of a cyberattack. One of the more vexing problems for policy in cybersecurity is that attack outcomes are hard to forecast in advance. Some attacks make mayhem, others collect information. Sometimes, it is not particularly certain that the attacker knows what the outcome will be. Consider the 2021 ransomware attack on Colonial Pipeline, an ostensible act of cybercrime. The intent of those who emplaced ransomware on Colonial's systems was to force a significant payout. Due to the way Colonial's systems failed, supplies of refined fuels such as gasoline, diesel, and jet fuel ceased flowing across much of the eastern United States. It appeared that the attackers knew there could be a sizeable payout, but it is hard to believe that they aimed to cause a massive alarm which would ripple across government and industry. Poor reconnaissance was to blame.

Our central case, the 2015 Ukraine power grid hack, was quite the opposite. From a variety of cybersecurity news sources and researchers, the details of how the attackers prepared to hit their targets dribbled out. Over the course of nearly a year prior to the attack, unknown actors clandestinely established persistent access to multiple industrial networks and identified targets. The attacking party employed spear phishing email to compromise networks of the oblenergos and install the BlackEnergy malware on their systems facilitating further unauthorized access to their networks. The attackers stole legitimate employee credentials used them to gain further access. VPN tools were employed to enter the Industrial Control System (ICS) network. Remote access tools issued commands to ICS computers. A modified version of the KillDisk malware, which deletes hard drives, also turned up on the compromised networks.

The Ukraine power grid hackers had a clear objective in mind, shut off power distribution, and possibly damage the grid for a long time. This has been an objective of Russia in its hot war in Ukraine which began in February 2022, however the primary weapons now employed are cruise and ballistic missiles. The 2015 attack entered its execution phase when computer systems began to fail and power stopped flowing. Lee, Assante, and Conway chronicled how it unfolded:

> [On] December 23, 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers. The outages were due to a third party's illegal entry into the company's computer and SCADA systems: Starting at approximately 3:35 p.m. local time, seven 110 kV and 23 35 kV substations were disconnected for three hours. Later statements indicated that the cyber attack impacted additional portions of the distribution grid and forced operators to switch to manual mode.[51]

When the attack began, the attackers were able to use remote access tools to issue commands directly from a remote station and communicate to devices allowing the attackers to access industrial computers responsible for managing the flow of electricity. This permitted them to remotely open circuit breakers, thus cutting off delivery of electricity. These connections also permitted manipulating or erasing firmware on control system computers, potentially crippling them (and possibly cutting power for days or weeks). Back-up power systems shut down to impact power grid load with a scheduled service outage. A telephone denial-of-service attack on the call center (launched from Russia) made it difficult for impacted oblenergos to receive notice from customers regarding outages. The three Ukrainian oblenergos experienced coordinated cyberattacks executed within 30 minutes of each other. The attack impacted 225,000 customers and required the oblenergos to move to manual operations in response to the attack. The oblenergos were able to restore service after an outage window lasting several hours.

In outlining a framework for geopolitically relevant cyber case study documentation, policymakers will inevitably be informed by PICCA framework outputs. These policy responses are beyond the scope of this article, but some caveats remain. Attribution is inherently difficult as nation-state and non-state actors may engage in false flag attacks and try to maintain plausible deniability. In the case of cyberattacks by nation-states and non-state actors, policymakers will consider concepts such as deterrence and appropriate instruments in their responses.[52] It is important to bear in mind that responses must be proportional and within the confines of international law and norms which is evolving in this issue area. By including an assessment of damage in the geopolitical context, the PICCA Framework lends itself to a proportional response analysis for policymakers.

Conclusion

This article presented the Policy Informative Cyber Case Analysis framework for qualitatively documenting geopolitically significant cyber-attacks in a structured fashion. The framework calls upon the analyst to *identify* the incident temporally, characterize the attack's reconnaissance and preparation, execution, and mitigation and resolution. Next is an assessment of the incident which includes assessing the code, reviewing open-source materials on the incident, and interviews with relevant subjects. Finally, the framework seeks the intent of the attack or incident which lends itself to attribution and the geopolitical significance of the event for policymakers. With case studies gathered, structured analytic techniques can then be applied to the cases to avoid misattribution and maintain the legitimacy of reporting agencies; a difficult yet important task in this era of misinformation, disinformation, information warfare, and digital influence attacks.[53] This article highlighted two structured analytic techniques this system lends itself to: Chronologies and timelines and devil's advocacy as discussed by Beebe and Pherson. This article used examples such as Russia's attack on the Ukrainian electrical grid in 2015 and Solar Winds to illustrate the utility of the framework.

The Policy Informative Cyber Case Analysis and the case studies generated from it, combined with the application of structured analytic techniques, will help nations, corporations, and civil society to better understand the chronology, modus operandi, and the geopolitical context and significance of the event. It will also help licit and state actors, interrogate assumptions about cyber-attacks to maintain trust and legitimacy in an era of information conflict. Much as with other forms of descriptive activity of international disputes or conflicts, cybersecurity requires a structure for communicating the salient features of each attack to a policy audience. This is a suggestion for how to structure that communication.

Endnotes

[1] Hatch, Benjamin B. "Defining a class of cyber weapons as WMD: An examination of the merits," *Journal of Strategic Security* 11, no. 1 (2018): 43-61, https://www.jstor.org/stable/10.2307/26466905.

[2] Jon R. Lindsay, “Stuxnet and the limits of cyber warfare.” *Security Studies* 22, no. 3 (2013): 365-404, https://doi.org/10.1080/09636412.2013.816122; Erik Gartzke, “The myth of cyberwar: bringing war in cyberspace back down to earth.” *International Security* 38, no. 2 (2013): 41-73, https://www.belfercenter.org/publication/myth-cyberwar-bringing-war-cyberspace-back-down-earth.

[3] Brandon Valeriano and Ryan C. Maness. *Cyber war versus cyber realities: Cyber conflict in the international system*. (New York: Oxford University Press, 2015).

[4] Blanken-Webb, Jane, Imani Palmer, Sarah-Elizabeth Deshaies, Nicholas C. Burbules, Roy H. Campbell, and Masooda Bashir. "A case study-based cybersecurity ethics curriculum." In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. 2018.

[5] Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." *IEEE Security & Privacy* 9, no. 3 (2011): 49-51, https://doi.org/10.1109/MSP.2011.67.

[6] Liu, Simon, and Bruce Cheng. "Cyberattacks: Why, what, who, and how." *IT Professional* 11, no. 3 (2009): 14-21.

[7] Chris Bronk, “Hacking the nation-state: Security, information technology and policies of assurance.” *Information Security Journal: A Global Perspective* 17, no. 3 (2008): 132-142, https://doi.org/10.1080/19393550802178565.

[8] Stephen Herzog, “Revisiting the Estonian cyber attacks: Digital threats and multinational responses,” *Journal of Strategic Security* 4, no. 2 (2011): 49-60, https://www.jstor.org/stable/10.2307/26463926.

[9] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata. “Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war.” *Security Dialogue* 43, no. 1 (2012): 3-24, https://doi.org/10.1177/0967010611431079.

[10] Christopher Bronk, and Eneken Tikk-Ringas. “The cyber attack on Saudi Aramco,” *Survival* 55, no. 2 (2013): 81-96, https://doi.org/10.1080/00396338.2013.784468.

[11] Jennifer Rowley, “Using case studies in research,” *Management Research News* 25, no. 1, (2002): 16-27, https://doi.org/10.1108/01409170210782990.

[12] Christine Benedichte Meyer, “A case in case study methodology,” *Field methods* 13, no. 4 (2001): 330, https://doi.org/10.1177/1525822X0101300402.

[13] Benedichte Meyer, “A case in case study methodology,” *330*.

[14] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, (Cambridge: MIT Press, 2005): 6-7; Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997), 51-52.

[15] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 75.

[16] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 67.

[17] George and Bennett, *Case Studies and Theory Development,* 13, where the authors cite the classic work of Gary King, Robert O. Keohane, and Sydney Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research* (Princeton: Princeton University Press, 1994).

[18] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 67.

[19] “Armed Conflict Location & Event Data Project (ACLED) Quick Guide to ACLED Data,” ACLED, June 2022, https://acleddata.com/acleddatanew//wp-content/uploads/dlm_uploads/2022/06/ACLED_GeneralUserGuide_June2022.pdf; Clionadh Raleigh, Andrew Linke, Håvard Hegre, and Joakim Karlsen, “Introducing ACLED-Armed Conflict Location and Event Data.” *Journal of Peace Research* 47 no. 5 (2010): 651-660, https://doi.org/10.1177%2F0022343310378914.

[20] Randolph Pherson, “The Five Habits of the Master Thinker,” *Journal of Strategic Security* 6, no. 3 (October 2013): 54–60, https://doi.org/10.5038/1944-0472.6.3.5.

[21] Randolph H. Pherson and Richards J. Heuer Jr, *Structured Analytic Techniques for Intelligence Analysis*, Third Edition (Thousand Oaks: CQ Press, 2021), 138-142.

[22] Pherson and Heuer, *Structured Analytic Techniques for Intelligence Analysis*, 141-142.

[23] Joe Devanny, Luiz Goldoni, and Breno Medeiros, “Strategy in an Uncertain Domain: Threat and Response in Cyberspace,” *Journal of Strategic Security* 15, no. 2 (July 1, 2022), 34, https://doi.org/10.5038/1944-0472.15.2.1954; Joseph S. Jr. Nye, “The End of Cyber-Anarchy?: How to Build a New Digital Order Digital Disorder,” *Foreign*

DOI: https://doi.org/10.5038/1944-0472.16.1.2068

Affairs 101, no. 1 (2022): 32–43, https://heinonline.org/HOL/P?h=hein.journals/fora101&i=34.

[24] Hassanzadeh, Amin, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M. Katherine Banks. "A review of cybersecurity incidents in the water sector." *Journal of Environmental Engineering* 146, no. 5 (2020): 03120003.

[25] Sarah Miller Beebe and Randolph H. Pherson, *Cases in Intelligence Analysis: Structured Analytic Techniques in Action* (Thousand Oaks: CQ Press, 2015), 43-58. See also Instructor's Materials pages 27-28.

[26] Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G. de Paula, Natasha Malara Borges, "A Case Study of the Capital One Data Breach (Revised)," *Cybersecurity Interdisciplinary Systems Laboratory, Massachusetts Institute of Technology*, March 2020, https://web.mit.edu/smadnick/www/wp/2020-16.pdf.

[27] Jason Healey and Karl Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, CCSA/Atlantic Council, 2013.

[28] Ryan Franklin Smith, Brian Coulson, and Dan Kaiser, "Using MITRE ATT&CK™ in Threat Hunting and Detection," LogRhythm Labs (United Kingdom: Mitre Corporation, 2018), www.logrhythm.com.

[29] Maymí, Fernando, Robert Bixler, Randolph Jones, and Scott Lathrop, "Towards a definition of cyberspace tactics, techniques and procedures," In *2017 IEEE International Conference on Big Data (Big Data)*, pp. 4674-4679. IEEE, 2017, https://doi.org/10.1109/BigData.2017.8258514.

[30] Ioannis Agrafiotis, Jason RC Nurse, Michael Goldsmith, Sadie Creese, and David Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity* 4, no. 1 (2018), https://doi.org/10.1093/cybsec/tyy006.

[31] Jerome H. Saltzer and Michael D. Schroeder. "The protection of information in computer systems." *Proceedings of the IEEE* 63, no. 9 (1975): 1278-1308, https://doi.org/10.1109/PROC.1975.9939.

[32] Thomas Rid and Ben Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37, https://doi.org/10.1080/01402390.2014.977382.

[33] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. "TRITON: The first ICS cyber attack on safety instrument systems," In *Proc. Black Hat USA*, vol. 2018, pp. 1-26. 2018.

[34] Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," *Wired,* August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[35] Joe Devanny, Luiz Goldoni, and Breno Medeiros, "Strategy in an Uncertain Domain: Threat and Response in Cyberspace," Journal of Strategic Security 15, no. 2 (July 1, 2022), https://doi.org/10.5038/1944-0472.15.2.1954.

[36] Zetter, Kim. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown, 2015.

[37] Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. "Computer Security Incident Response Teams (CSIRTs): An Overview." *The Global Cyber Security Capacity Centre* (2014).

[38] Rid, Thomas, and Ben Buchanan. "Attributing cyber attacks." *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37 and Egloff, Florian J., and Max Smeets. "Publicly attributing cyber attacks: a framework." *Journal of Strategic Studies* (2021): 1-32.

[39] Willett, Marcus. "Lessons of the SolarWinds hack." *Survival*63, no. 2 (2021): 7-26.

[40] "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," *FIREEYE*, December 13, 2020, https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

[41] Jenni Bergal, "Florida Hack Exposes Danger to Water Systems," Pew, March 10, 2021, https://pew.org/3btxWBc.

[42] Robert Grubbs, Jeremiah Stoddard, Sarah Freeman, and Ron Fisher, "Evolution and Trends of Industrial Control System Cyber Incidents since 2017," *Journal of Critical Infrastructure Policy* 2, no. 2 (2021), https://doi.org/10.18278/jcip.2.2.4.

[43] William Casey, Jose A. Morales, Thomson Nguyen, Jonathan Spring, Rhiannon Weaver, Evan Wright, Leigh Metcalf, and Bud Mishra, "Cyber security via signaling games: Toward a science of cyber security," In *International Conference on Distributed Computing and Internet Technology*, pp. 34-42. Springer, Cham, 2014.

[44] Rafał Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective." *Computers & Security* 108 (2021), https://doi.org/10.1016/j.cose.2021.102376.

[45] Doynikova, Elena, Andrey Fedorchenko, and Igor Kotenko. "Ontology of metrics for cyber security assessment." In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1-8. 2019.

[46] Facchinetti, Silvia, Paolo Giudici, and Silvia Angela Osmetti. "Cyber risk measurement with ordinal data." Statistical Methods & Applications 29 (2020): 173-185.

[47] Lavi Lazarovitz, "Deconstructing the SolarWinds breach," *Computer Fraud & Security* 2021, no. 6 (2021): 17-19, https://doi.org/10.1016/S1361-3723(21)00065-8.

[48] Carley, Kathleen M. "Social cybersecurity: an emerging science." *Computational and mathematical organization theory* 26, no. 4 (2020): 365-381.

[49] Ioannis Agrafiotis, Jason RC Nurse, Michael Goldsmith, Sadie Creese, and David Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity* 4, no. 1 (2018), https://doi.org/10.1093/cybsec/tyy006.

[50] Bhawna Narwal, Amar Kumar Mohapatra, and Kaleem Ahmed Usmani, "Towards a taxonomy of cyber threats against target applications," *Journal of Statistics and Management Systems* 22, no. 2 (2019): 301-325, https://doi.org/10.1080/09720510.2019.1580907.

[51] Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," Traffick Light Protocol: White (Washington, D.C.: SANS, March 18, 2016): 1, https://nsarchive.gwu.edu/document/15331-sans-and-electricity-information-sharing-and.

[52] Nye Jr, Joseph S. "The End of Cyber-Anarchy?: How to Build a New Digital Order." *Foreign Affairs* 101 (2022): 32.

[53] James J. F. Forest, "Political Warfare and Propaganda: An Introduction," *Journal of Advanced Military Studies* 12, no. 1 (Spring 2021): 3, 14, https://doi.org/10.21140/mcuj.20211201001.