The University of Chicago

Local Solutions to National Security Challenges: Bridging the Center-Periphery Information Sharing Gap

by Max Markusen

August 2021

A paper submitted in partial fulfillment of the requirements for the Master of Arts degree in the Master of Arts Program in the Committee on International Relations

Faculty Advisor: Austin Carson
Preceptor: Nick Campbell-Seremetis

ABSTRACT

An enduring feature of politics and international security is the ability of nation states to respond to transnational threats. National governments often share protected information on these threats, especially when sharing such information would pre-empt a national security crisis. Inevitably, however, the failure of nation states to share information can lead to catastrophic disaster. While previous research has focused on intelligence and information sharing between nation states (international information sharing), and within national government organizations (intragovernmental information sharing), this thesis is primarily concerned with sharing information across tiered levels within nation states, in particular between national governments and local governments (i.e., center-periphery information sharing).

This thesis applies the center-periphery lens to the problem of information sharing, and points to the role of organizational bureaucracies as a key mechanism in enabling or obstructing the flow of information both from the center to the periphery (i.e., top-down information sharing), and from the periphery to the center (i.e., bottom-up information sharing). Organizations often overcome gaps that individuals have in failing to share information, but can also play a pivotal and sometimes detrimental role in preventing information from flowing between national and local partners. This thesis uses both historical and contemporary case studies to illustrate center-periphery information sharing challenges around the world, both from the national level to the local level, and from the local level to the national level.

A key takeaway from the study of center-periphery information sharing is the concept that the power of a nation state goes beyond national government—including executive, legislative, and judicial branches—and extends to local governments and organizations. A nation-state's power is held at the local level, and oftentimes early warnings about national

security issues are predicted by national government organizations, but by local organizations at the periphery. Whether national and local partners face threats from cybercrime, transnational terrorism, or corporate espionage, this center-periphery information sharing lens illustrates how events at the local level impact national statecraft.

SECTION I: Introduction, Background, and Relevance

Introduction: On January 6, 2021, a mob of protestors breached a secure perimeter around the U.S. Capitol Building and stormed onto the floor of the most influential legislative chamber in the world. The U.S. Capitol police officers and D.C. Metropolitan police officers on duty to protect the Capitol were underprepared and quickly overwhelmed. 140 officers—73 Capitol Police and 65 D.C. Metropolitan police—were injured during the attacks, including the death of a Capitol police officer, and later, two suicides by D.C. Metro police officers.

Around twelve percent of the protestors were members of right-wing militia groups or white nationalist organizations, and the mob included a disproportionately large percentage of current and former members of the U.S. military.[1] According to an ongoing University of Chicago study by the Chicago Project on Security and Threats (CPOST), of the 444 total arrested participants in the January 6 attacks, at least 61 participants—13 percent—were confirmed current or former members of the U.S. military. CPOST data show that of these 61 confirmed military affiliations, 28 percent were in militia groups (nine Proud Boys, six Oath Keepers, one member of the Three Percenters, and one Aryan Nations).[2] As a point of reference, approximately 7 percent of the adult population are U.S. military veterans,[3] making the total

[1] CPOST data current as of 14 May 2021. https://cpost.uchicago.edu/research/domestic_extremism/
[2] CPOST data current as of 14 May 2021. https://cpost.uchicago.edu/research/domestic_extremism/
[3] U.S. Census. https://www.census.gov/library/publications/2020/demo/acs-43.html

number of veterans at the Capitol Hill insurrection nearly twice the national average of men and women who have served in uniform.

In the wake of these attacks, policymakers and pundits have questioned whether the U.S. Capitol Police had sufficient intelligence indicating whether an attack was about to take place, or if not, whether the U.S. intelligence community failed to share this information, or whether they failed to predict the incident itself. A recent Senate report found that while U.S. Capitol police claimed to have no pre-warning of the attacks, a January 5 FBI situational information report warned of impending violence at the Capitol.[4] This report cited social media posts encouraging protestors to "bring guns" and "storm the Capitol." This report was shared at the center of the U.S. government, but not with local partners on the periphery. The FBI shared this information with a limited number of partners, including by email with a limited audience at the U.S. Capitol Police, but no other significant steps were taken to share details of the impending violence with local partners defending the Capitol, including Washington D.C. Metropolitan police, or with the D.C. National Guard. The limited amount of information sharing between the center and the periphery that took place did nothing to impede the attacks the following day, which would leave the United States, and indeed the world, reeling on shock at the photo and video footage of the U.S. Capitol under attack.

Halfway around the world, a different crisis is taking shape, one that can be analyzed through the same center-periphery lens. In the Chinese province of Xinjiang, the Chinese national government is approaching a similar information sharing problem in a much different way. In response to real and perceived terrorist threats from the Uyghurs—a Muslim ethnic minority group in China—Chinese domestic surveillance of ethnic Uyghurs has increased

[4] Joint U.S. Senate Committee Report on "Examining the U.S. Capitol Attack: A Review of the Security, Planning, and Response Failures on January 6."

dramatically, resulting in hard crackdowns including concentration camps for alleged "re-education purposes."

Chinese authorities collect intelligence about local threats at the periphery, rather than at the center of the government. Local Chinese authorities implement technological surveillance at the local level, using indicators and warnings that are automated on a system built by a private company called Landasoft. The Chinese government deploys this software and pushes reports to local police for investigation. The Chinese government claim that this software powers a law enforcement system that has successfully foiled attacks. Obviously, the situation in Xinjiang raises major ethical and moral concerns, but nonetheless illustrates how government organizational bureaucracies can bridge the center-periphery information sharing divide, resulting in better information flow, albeit for authoritarian regimes taking the most terrible and reprehensible steps in the name of information sharing.

The two vignettes above are examples of how information and intelligence can successfully be shared—and fail to be shared—between national and local levels at the center and the periphery of a government. Most of the existing academic literature on information sharing focuses on intelligence failures at the international levels (for example, between the United States and United Kingdom on transnational terrorist threats), and at the intragovernmental levels (i.e., failures by the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) to share information with one another). Far too often, we hear about failed information sharing when it results in a catastrophic disaster, and often this is a failure of international or intragovernmental information sharing. However, there are many instances of intelligence information failing to flow from the center to the periphery, and vice

versa. This failure of information sharing between national and local entities is the focus of this paper.

This paper seeks to extend the literature on intelligence failures by going beyond the traditional explanations of international information sharing and intragovernmental information sharing and seeks explain the phenomenon of information sharing up and down levels of national, state, and local government. It seeks to explore intelligence failures between national governments or federal agencies, and local governments or localized agencies. This paper refers to this type of information sharing as *center-periphery information sharing.* Much like the failures of intergovernmental and intragovernmental information sharing, examples of successful and failed center-periphery information sharing span topics from terrorist attacks, domestic political violence, cyber-attacks on public and private targets, maritime disasters, infrastructure vulnerabilities—to name a few.

The cases in this paper will demonstrate failures of information flowing form the local to the national levels (i.e., from the periphery to the center) as well as from the national level to the local level (i.e., from the center to the periphery). While the nature of this thesis project limits the scope of this paper, there are many other examples of center-periphery information sharing in the United States and around the world. Nor is this phenomenon exclusively a feature of modern history. National governments have long faced challenges to sharing information or intelligence across the center-periphery divide. Ancient examples of center-periphery information sharing failures may including the failure to properly warn and put an end to the crescendo of slave revolts that took place across the Roman empire leading to the three Servile Wars (135-132 BC; 104-100 BC; 73-71 BC). An entire study could be done on the center-periphery information sharing failures during ancient empires, including extending to problems with information

flowing between the center and periphery during Roman, Greek, or even ancient Chinese societies. However, a reliable academic study would be challenged to find credible historical sources, including primary documents that go beyond myths and stories passed down through oral traditions.

Relevance: This paper has four major relevant contributions: to theory about how power is distributed across a state; to understanding how states assess domestic vulnerability and defend against threats internal to nation states; to understanding how states respond to international or transnational threats; and to how governments might better wage low-intensity conflicts like counterterrorism campaigns or counterinsurgencies, where local information is critical for understanding conflict and crafting successful national policies.

First, the study of center-periphery information sharing seeks contributes to the field of political science by expanding academic understanding of how power is given and distributed across the national and local levels of a nation-state. The literature on intelligence failures shows that government decisions at the national level have grave consequences for national security, but this paper seeks to show that government decisions at the local level also have grave consequences for national security.

The study of center-periphery in social sciences has looked at how economic power of a state can be projected from the periphery as well as from the center, or the core. This paper seeks to build on Immanuel Wallerstein's conceptualization of the core, periphery, and semi-periphery in the world capitalist system.[5] While Wallerstein uses this lens to conceptualize how power is broken across the international system, this paper seeks to use this lens to demonstrate how other categories of power like military, diplomatic, and intelligence can also be projected across the

[5] Wallerstein, Immanuel. (1974). "The Rise and Future Demise of the World Capitalist System: Concepts for Comparative Analysis." *Comparative Studies in Society and History, 16(4).* pp. 387-415.

center-periphery divide. Center-periphery information sharing failures help illustrate this theory, supporting the claim that power of a nation-state is generated at the local level—when information fails to flow from the local level to the national level, or vice versa, there may be grave consequences for national security and real implications for the power of a nation state.

Second, this paper shows that successful center-periphery information sharing is critical for assessing domestic vulnerability and threats within a nation state. This is even more important in an interconnected world where nation states are contending with unprecedented threats across the spectrum of national power. Failures of center-periphery information sharing can result in mischaracterizing internal vulnerabilities like election systems, and critical infrastructure. Therefore, understanding center-periphery information sharing has policy implications for understanding how governments apply national level information sharing resources to local problems, and how nations might apply some of the proven bureaucratic mechanisms developed for international information sharing and intragovernmental information sharing to better address gaps or blockages in center-periphery information sharing.

Third, the study of center-periphery information sharing is not only relevant to how nation-states assess internal security threats, but also to understanding how nations share information from the center to the periphery (and vice-versa) on international and transnational threats. While failure to stop terrorist attacks are traditionally looked at through the lens of international information sharing and intragovernmental information sharing, failures of center-periphery information sharing can contribute to failures to stop catastrophic transnational terrorist events including the September 11 terrorist attacks, Boston Marathon bombings, London subway bombings, or attack on the Bataclan, Charlie Hebdo, and others. Moreover, as recent transnational crises have shown, international terrorism is not the only transnational threat states

face in the 21st century. This thesis will examine a case study of the recent ransomware cyber-attacks on Colonial Pipeline as an example of how the failure of information sharing between the center and the periphery inside a nation-state can result in a catastrophic event.

A related contribution of the study of center-periphery information sharing is toward understanding how governments wage low intensity conflict, including counterinsurgency, or COIN campaigns. A critical component of COIN is getting information from local partners (local leaders, intelligence sources, and informants), to different national partners (military and law enforcement). This concept illustrates the importance of center-periphery information sharing, and this paper will look at a case study on the French-Algerian War to illustrate how center-periphery information sharing failures can lead to setbacks or even failures of counterinsurgency campaigns.

For any information-based counterinsurgency strategy to succeed, national powers at the center need to get information from the periphery at the local level (i.e., bottom-up), but national-level information also needs to flow from the center out to the periphery. For example, in targeting of counterinsurgencies, if there is a lack of bureaucratic structures, there is a lack of information fusion. This was a problem for the U.S. military community in the early years after 9/11 and the invasions of Iraq and Afghanistan. However, the U.S. special operations community has come up with novel international, intragovernmental, and even center-periphery information-sharing solutions through bureaucratic mechanisms at U.S. Special Operations Command (USSOCOM) and Joint Special Operations Command (JSOC).

Definition of Terms: This paper uses several key terms that characterize the types of information sharing and help place this thesis in the broader literature on information sharing.

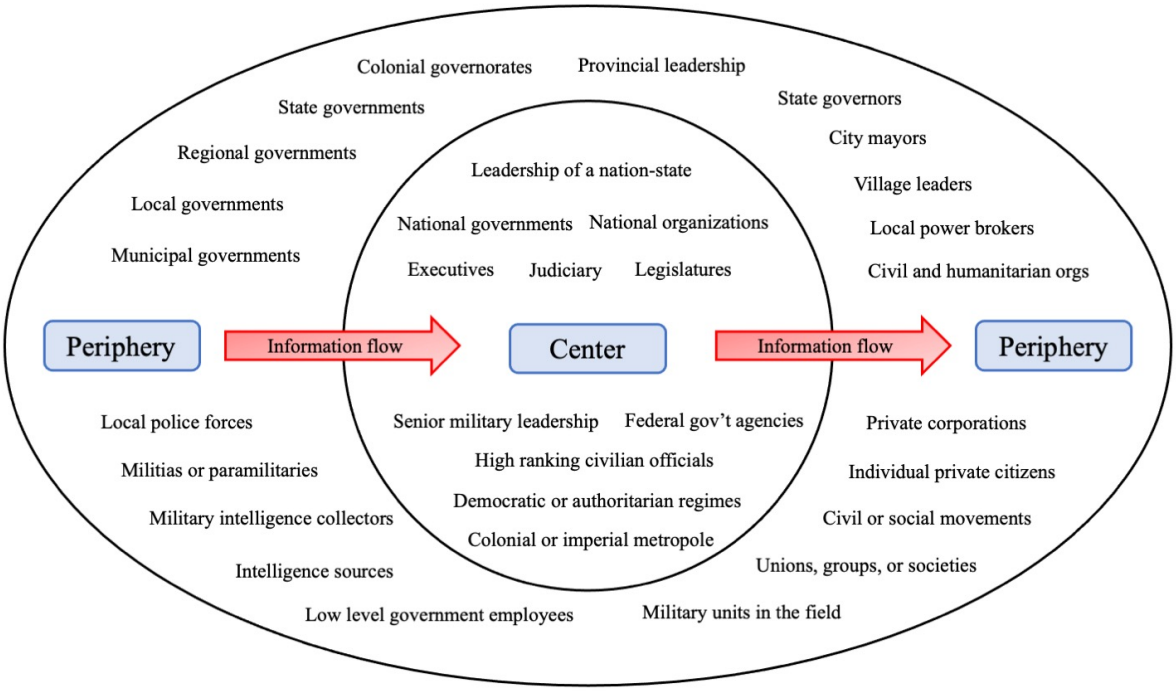
First is a term that this paper uses to describe intelligence and information sharing that takes place between nations. This paper refers to this phenomenon as *international information sharing*, which usually takes place among allies or international bureaucratic mechanisms. For the United States, a common example of international information sharing would be the FIVE EYES (FVEY) partnership, which is an intelligence sharing mechanism between the countries of the United States, U.K., Canada, Australia, and New Zealand. Nation states also participate in information sharing with international bureaucratic organizations like the International Atomic Energy Agency (IAEA), or with international law enforcement agencies like INTERPOL.

The second broad type of intelligence and information sharing that this paper discusses is the sharing that takes place among agencies or organizations within national governments. This paper refers to this as *intragovernmental information sharing*, which usually takes place between or among federal government agencies. A common example in the United States would be the State Department and the Defense Department sharing cables or messages from foreign embassies about the state of play with a foreign ally or enemy. The United States also has bureaucratic mechanisms to share intragovernmental information, like the U.S. National Counterterrorism Center (NCTC), which shares information on terrorist threats to the United States. France has a similar organization known as the French National Oversight Commission for Intelligence Gathering Techniques (CNCTR). In addition to sharing information between national government agencies, intragovernmental information may also take place between branches of national government like executive and legislative branches of a federal government.

Third, this thesis seeks to introduce a new concept into the literature on information sharing that describes instances when national government entities share information with local partners or local government entities. This paper uses the term *center-periphery information*

sharing to describe this phenomenon, but also considered other terms including "federal-local," "national-local," "multi-tiered," and "cross-level." All these terms get to the fundamental nature of the problem—information crossing up and down from national governments (the center) to local governments (the periphery), but the term "center-periphery" encompasses them all, and draws on previous literature about the center-periphery divide. Figure One below is a chart illustrating the flow of center-periphery information sharing. Note how information flows both from the periphery to center, as well as from the center to the periphery.

Figure One: Center-Periphery Information Sharing Flow



The center-periphery model is a spatial metaphor that has been used in other social science research, including Wallerstein (1974). In this case, the center-periphery relationship may include information sharing flowing from the local-level to the national-level (i.e., bottom-

up), or information flowing from the national-level to the local-level (i.e., top-down). It can happen between national and state and local partners, but as this thesis will illustrate, it can also happen between a colonial metropole and a colonial governor or village leader. Non-federal systems like China also have examples of center-periphery information sharing, as is the case with the Landasoft public-private partnership to use technology platforms to monitor Uighyers in Xinjiang province.

Some examples of contemporary center-periphery information sharing occur in the United States at the FBI's Joint Terrorism Task Forces, or in the U.K.'s National Counter Terrorism Policing Network. As a result of the threat of terrorism in the 21st century, this center-periphery information sharing often takes place around terrorist threats, but examples extend into other fields like the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) which has a National Infrastructure Coordinating Center (NICC). Legally, this entity is required to share information on infrastructure threats with U.S. state and local partners. In practice, however, it does not work so perfectly.

This paper also uses terms like *national government* to refer to the role of the nation state, as separate and distinct as the governing structures at the state and local level. National governments would include any internationally recognized government—including both federal and authoritarian systems—overseeing an entire nation or state (i.e., USA, UK, Russia, China), but also may include colonial or imperial powers, as separate and distinct from their colonial subjugates (i.e., British Crown, French Colonial System). On the other hand, this paper variously refers to *sub-national governments* and *state or local governments*, to refer to a local government, or a local governing structure at the level below an internationally recognized national government (i.e., New York State, the City of Los Angeles, British territories, French-

governed Algeria). For the purposes of this paper, we are interested in information sharing that goes between national governments and sub-national governments, i.e., between the center and the periphery.

SECTION II: Research Question and Possible Explanations

Research Question: There are many ways to explore the topic of center-periphery information sharing. This study considered questions including categories of reasons why national governments decide to share information with local governments; categories of mechanisms national governments use to share information with sub-national governments; whether timing has a role in information sharing; and the types of recipients of information that a national government shares this information with, for example, regional, governorate, state, district, and local authorities, or even private corporations.

This thesis, however, is primarily concerned with the mechanisms for center-periphery information sharing, and why shared information can be discarded or ignored, even if information is shared between the center and the periphery.

Roles of Individuals and Organizations: Some scholars may argue that it's individuals who play an important role in information sharing or blocking information sharing between the center and the periphery. Indeed, these case studies will show that individuals play important roles in center-periphery information sharing, whether it's the Colonial Pipeline CEO or the French military intelligence officer on the ground in Algeria. Individuals make up organizations, so it's natural to think that center-periphery information sharing can be explained through the exploration of the role of the individual. Disgruntled civil employees or military service members can leak information to jump the chain of command, or politicians with certain

information may decide to go public if it's politically expedient. Individuals, especially human sources of information, are vital for information to make it into the system in the first place. We may point to the fact that senior leaders at the center may disregard information from unreliable human sources, or that information from shoddy sources on the periphery don't get shared in the first place.

However, the research in this paper demonstrates that—regardless of the role of the individual—in most, if not all cases, there is an organizational or bureaucratic mechanism involved in most information sharing, and oftentimes plays a critical role in the success and failure of this type of information sharing—both from the bottom-up and the top-down. In some cases, bureaucracies pose a challenge to center-periphery information sharing, and sometimes bureaucracies play a critical role in overcoming problems with this type of information sharing.

Moreover, the importance of the role of individuals can be explained away by organizations and bureaucracies. The reasons individuals play important roles always tie back to bureaucratic organizational explanations, either through an attempt to circumvent the bureaucracy, participating in a critical bureaucratic information sharing mechanism, or getting foiled by a bureaucratic mechanism that prevents information sharing. For example, a disgruntled employee who leaks or shares classified information; or an individual who withholds information for politically expedient reasons. In both cases, individual motivations can be tied back to organizational explanations. A desire to leak information is tied to dissatisfaction with current organizational mechanisms, and a desire to withhold may be tied to organization completion for resources, or an individual trying to "cover their own ass" to retain promotion potential. This psychological analysis of individual decision to withhold or share information exceeds the scope of this paper but can be tied back to explanations from the organization.

This paper will show that regardless of individuals and their motivations, problems with center-periphery information sharing can usually tie back to the presence of some bureaucratic organizations. Previous research on information sharing shows that bureaucracies play a critical role in both international and intragovernmental information sharing, and this paper will extend this literature to center-periphery information sharing.

The core argument of this paper is that organizations play a critical role in both sharing and withholding information. These organizations most commonly occur as bureaucracies, and this explanation in this paper will also be referred to as an explanation from bureaucratic mechanisms. Successful center-periphery information sharing can take the form of pre-established bureaucratic mechanisms, including legal mandates to share, or information sharing organizations. Center-periphery information sharing failures can also be explained by poor or missing bureaucratic mechanisms, or legal limits on the ability to share.

Possible Explanations: The research in this paper will show that information flowing from the center to the periphery (i.e., top down) often fails when a bureaucratic structure is missing, or when there are too many organizations at the periphery to share information with. This is the case with the Colonial Pipeline hack, and the inability of the United States government to properly convey threat levels and provide response capabilities to all private U.S. companies managing critical U.S. infrastructure. Conversely, this paper will show that when information is flowing from the periphery to the center, failures to act on information are usually a result of a disconnect between the center and the periphery on the understanding of the situation at the periphery. This was the case in Algeria in 1955, when the French colonial government simply could not conceive of the threats posed by the ALN and NLF at the periphery of the colonial system.

This paper will be primarily concerned with center-periphery information sharing failures, and by doing so, will build on a larger body of work about the role of bureaucracies in information and intelligence sharing failures. The case studies in this paper will attempt to explain how organizations interact with information sharing from the center to the periphery (i.e., top down), as well as from the periphery to the center (i.e., bottom up). The case of French Algeria will show that despite information sharing mechanisms (military chain of command), the parochial view from the center prevented it from acting on good information from the periphery. These parochial viewpoints from the center can prevent it from acting on periphery information. Similarly, the case of Colonial Pipeline will show that information traveling from the center to the periphery can fail if there are too many organizations the periphery, and/or if a bureaucratic mechanism is not effective in disseminating this information.

Organizations and Information Sharing: There are two sets of key variables to consider when characterizing the role that organizational bureaucracies play in center-periphery information sharing: sharing vs. withholding; and intentional vs. unintentional. These variables are illustrated in **Figure Two.**

Sharing vs. Withholding: Simply put, center-periphery information sharing either happens or it doesn't. Information is shared between the center and the periphery, or it is withheld. However, sometimes when information is shared, it is not acted upon. This paper is primarily interested in instances where information is shared between the center and periphery—either intentionally or unintentionally. Instances in which information is shared between the center and the periphery is valuable in illustrating the importance of information sharing, and the impact of local governments on nation-state decision making, but successful information sharing is a secondary focus of this paper. The case studies in this paper will focus on examples of

organizational bureaucracies failing to share information, either through intentional withhold, unintentional withhold, or whether these bureaucracies are missing altogether.

Intentional vs. Unintentional: As alluded to above, instances in which information is withheld between the center and the periphery may include both intentional and unintentional withholding of information. Organizations and bureaucracies play a role in both types of withholding. For example, an unnecessarily large bureaucracy may unintentionally impede communications, resulting in unintentional withholding. On the other hand, resource rivalry between bureaucracies may result in intentional withholding.

Figure Two is a 2x2 table that categorizes the types of organizational roles for center-periphery information sharing. This thesis is primarily concerned with bureaucratic role in withholding information, but the 2x2 table also demonstrates how bureaucracies share information.

Figure Two: Organizational Roles in Center-Periphery Information Sharing

	Intentional	**Unintentional**
Withhold	I. Intentionally withholding information: • Information protection • Legal limits on sharing • Organizational rivalries • Coveting information, or "need to know" policies • Intentional obfuscation • Resource rivalry	II. Unintentionally withholding information: • Bureaucratic disfunction leading to accidental withhold of information • Communications breakdowns • Lack of resources (manpower, money) • Failure to organize despite forewarning
Share	III. Intentionally sharing information: • Legal mandates to share • Organizations set up to share • Political incentives/expediency • Breaking the rules to share	IV. Unintentionally sharing information: • Accidental leak of information or data spillage • Shared sources of information

The table above helps to categorize cases for specific explanations. For example, Quadrant I provides explanations on why information protection takes place, suggesting that

these kinds of activities are more likely to prevent information sharing. It also suggests that where there is bureaucratic rivalry, it's more likely to prevent information sharing. Quadrant II illustrates situations in which there are accidental breakdowns, providing some insight into how better policy could shape center-periphery information sharing. Quadrant III illustrates examples of cases where there might be problems with individuals, but the organization or bureaucracy helped get through information sharing problems. Further exploring these categories and cross-referencing this 2x2 table with a large number of cases to each type of category would provide for a rich expanded study on the topic.

SECTION III: Literature Review

This paper will be primarily concerned with center-periphery information sharing failures, and by doing so, will build on a larger body of work about information and intelligence sharing failures. Interestingly, while there is literature on the instances in which states share information across international bureaucracies, this phenomenon is relatively rare due to state secrets and sovereignty. Conversely, there is a lot of intragovernmental information sharing that takes place within central/national governments, and a healthy amount of literature on the subject, particularly in the post-9/11 environment with high threats of transnational terrorism. However, there is virtually no literature on information sharing that takes place within nation-states, including center-periphery information sharing, which happens even more frequently, making this a vast gap in the literature.

This literature review below is split into several different levels of analysis: literature on explanations for international information sharing; existing literature on intragovernmental information sharing; a short review of literature on center-periphery information sharing; and a

brief overview of the psychological and management literature on why leaders of organizations use information sharing to build stronger organizations, particularly within companies.

Literature on International Information Sharing: The role of information sharing on the international stage has been widely studied, including why governments withhold information, how governments decide to share information with allies, partners, and adversaries to increase leverage and bargaining power; how governments share intelligence with partners to increase collective security; how governments share information with international organizations ensure compliance for trade and weapons violations (Carnegie and Carson, 2020); how governments conceal information from the public to save face (McManus and Yarhi Milo 2017); and how governments reveal information to adversaries to signal clandestine capabilities or to deter action (Carson and Yarhi Milo, 2017).

However, this type of information sharing is relatively rare, and usually takes place when a massive transnational crisis is about to take place, or between allies preventing strategic adversaries from acquiring advantages, like nuclear weapons. However, even if international information sharing is relatively rare, this literature is still relevant. This paper seeks to draw on these explanations and extend them to theories of center-periphery information sharing. For example, how failures to act on information shared from the periphery to the center might be a result of the organizations at the center trying to save face. For example, the French Algerian colonial leadership failing to act on prior intelligence about FLN attacks because they refused to believe that the ALN and FLN posed a threat to the French government. Similarly, how the FBI concealed pre-knowledge of right-wing extremist attacks in the 1960's because they were using sources from inside the KKK, and revealing these sources would be damaging to its credibility.

Literature on Intragovernmental Information Sharing: Work has also been done on intragovernmental information sharing, including failures to share information within bureaucracies (Zegart), and examining increased coordination between national intelligence agencies. This latter category includes United States post 9/11, as well as intelligence failures for terrorist attacks around the world, or on the failure by government agencies to properly attribute threats or make accurate assessments about intelligence abroad. These articles often implicitly assume that national governments are a black box of information and assume unified governance across nation states. This is a problem because this literature does not conceptualize levels below national level. This literature focuses on intrastate information sharing at national level, for example, stove piping between government agencies, and do not get into details about information sharing from the center of a government to its periphery.

Literature on Center-Periphery Information Sharing: Only a small amount of literature has generalized or drawn theories about center-periphery information sharing within nations, however, there is research on specific examples of successful and failed information sharing that can be extended to the center-periphery model. Scholars have suggested that the post 9/11 era is the first time when national level intelligence has been forced to coordinate with state or local police (Cordner and Scarborough, 2010).

This body of work mostly studies terrorist threats to states (i.e., FBI sharing intelligence on Al Qaeda targets with NYPD), but also looks at the role of national level intelligence in ensuring state security against foreign adversaries (FBI working with the U.S. private sector to prevent technology theft by China). Government documents showed that CIA and FBI failed to share intelligence and missed 23 opportunities to disrupt the 9/11 attacks. Why did these intelligence agencies fail to capture these attacks? The 9/11 report highlighted many areas for

further study, yet there are more contemporary examples of failures in preventing attacks. A RAND study concluded that intelligence agencies generated initial clues for only 14 percent of foiled or executed terrorist attacks, while federal law enforcement generated initial clues for around 25 percent of all terrorist attacks. By comparison, state and local police generated initial clues for around 11 percent of all terrorist attacks.

Some of this research help explain why governments share intelligence with state and local partners to increase collective security, but governments don't withhold intelligence from state and local partners because of a security dilemma. They may, however, have security concerns when sharing information with state and local partners, especially if they want to protect sources and methods, but don't have the requisite protections in place prior to sharing the information. This presents an opportunity for this paper to introduce the center-periphery lens of analysis to explain how decisions by organizations at the center or at the periphery drive the information flow between both sides.

Literature on Leadership Management Reasons for Information Sharing: Lastly, an area to further expand on for future study is the literature on why leaders share or withhold information. Graham Allison's literature on bureaucratic rivalry may help explain some of the reasons organizations fail to share. The literature on the "cult of the offensive" prior to World War I (Van Evera, 1984) and literature on group think could also explain how pre-conceived notions and institutional bias plays into reasons organizations share information, process information, withhold information, and/or fail to act on information. All this literature should be considered for future study to help further explain why leadership at the center may not take heed of information shared from the periphery, or why leaders at the center fail to effectively share information with organizations existing at the periphery.

SECTION IV: Argument and Methodology

This research project will take a qualitative research approach, assessing two "skinny" case studies, and drawing conclusions. There is vast opportunity for this study to be expanded, including the two introductory cases at the start of this paper—the January 6 Capitol Hill Insurrection, and the Chinese suppression of Uighurs in Xinjiang Province.

This cases in this paper will be primarily concerned with center-periphery information sharing failures—both when information was passed but was failed to be heeded, or when information fails to be shared altogether. In an attempt to assess this question this research project will examine two case studies in which national governments failed to share intelligence or information on an "impending attack" with sub-national government units (as was the case in the Colonial Pipeline hack), or where information about an impending attack failed to make it from the periphery back to the center of a nation-state (as was the case in the Battle of Philippeville).

Dependent Variable: Success or failure to share intelligence generally results in preventing or failing to prevent an attack. The success or failure of "an attack" will serve as the dependent variable. The wide range of possible cases could exhibit variation in the kinds of attacks, which could include but are not limited to terrorist attacks, domestic political violence, insurgencies, cyber-attacks on public and private targets, maritime disasters, and infrastructure attacks. Normally measuring success as an outcome can be difficult, but in this case of information sharing, it's relatively straightforward (i.e., evidence that information was shared to stop an attack; or evidence that information was withheld, and an attack was not stopped). Moreover, in the cases this thesis will assess, it will be plainly clear that information was shared

(or failed to be shared), and that this information had a determinable effect on the outcome of the attacks.

Independent Variable: I will look for cases in which organizations played a critical role in either withholding or ignoring information. For these cases, the participation of the bureaucracy in the failure to share or heed intelligence will serve as the independent variable. This may include organizations and bureaucracies upholding mechanisms for center-periphery information sharing, intentionally withholding information, unintentionally withholding information, and even unintentional sharing of information. In the absence of other explanations, we point to bureaucracy as a definitive factor in center-periphery case studies that exhibited failure to share, intentional withholding, or unintentional withholding. In the case of the Battle of Philippeville, for example, bureaucratic groupthink and physical distance from the information provided by the sources on the ground led to a disregard of the intelligence about the impending attack.

Hypothesis: In cases where information fails to flow from the center to the periphery (i.e., top-down), I hypothesize that organizations play a role in one of two ways. Either the organizations are underequipped to communicate across the vast physical gap to the periphery, or there are too many organizations at the periphery for the center to properly communicate with. In cases where information is flowing from the periphery to the center (i.e., bottom-up), I hypothesize that information is not shared, or not heeded if that information flowing to the center does not fit the organizational preconceived notions at the center, or if that information from the periphery is not immediately relevant to the organizations at the center.

Predictions: The research might show that sometimes bureaucracies are incapable of sharing information, or properly interpreting information, either because of limits of the

organization, or because of lack of perspective. While not the primary focus of this thesis, an expanded study on successful center-periphery information sharing might show that there are certain bureaucratic organizations that more easily moves between local and national level, and perhaps that helps with information sharing. The research might also show that individuals will likely have an impact on the way bureaucratic mechanisms engage in center-periphery information sharing. For example, individuals are more likely to be engaged in intentional withholding and intentional sharing, while in the absence of individual personalities, the bureaucracy might be more likely to share.

As discussed above, individuals may play critical roles to overcome bureaucratic problems, including cases where individual politicians or policymakers who intentionally prevented information from being shared, or an individual who did move quickly enough to share early warning signals. As outlined in Section II, however, I would predict that individuals' role in information sharing between center and periphery levels will tie back to bureaucratic explanations for information sharing.

SECTION V: Case Studies

Case Selection: Cases should illustrate information flow between the center and the periphery, demonstrating some of the mechanisms from the table above that withhold information—either intentionally or unintentionally, but must show clear evidence of a bureaucracy involved in unsuccessful information sharing between the center and the periphery. Selected cases should clearly show whether information was unsuccessfully shared from the bottom-up or from the top-down. In some cases, both directions may be illustrated. These cases could show that information sharing might be less successful when flowing from the bottom-up,

or perhaps the cases might illustrate that information sharing is more successful when traveling from the top-down.

Case Variation: Case studies for this thesis will not be varied on the outcome of the information sharing—but an expanded study may look at cases with a variation on whether center-periphery information sharing was both successful and unsuccessful. The cases in this study should exhibit variation on intentional and unintentional withholding, per Figure Two. As mentioned above, cases should be varied on the flow of information sharing. One will show the role of the bureaucracy in sharing information from the top-down, and one from the bottom up.

In both cases, I expect that the empirics will show that bureaucratic mechanisms play a definitive role in both sharing and withholding information from the center to the periphery. To this end, there are many cases that this thesis could have considered, including intelligence warnings about terrorist attacks, information sharing on cyber and infrastructure threats, information sharing from low-level election officials up to higher levels of the U.S. election system; local intelligence that could have pre-empted the outbreak of war, and more. Per the section above, this thesis looks at one U.S. case and one foreign case, one of which was an example of center-periphery information sharing from the bottom up, and one example of information sharing from the top down.

Case Study #1: Colonial Pipeline Hack

Note: For the purposes of this thesis, the author chose a timely U.S. case that also has relevant policy implications. The Colonial Pipeline case below highlights bureaucratic failures in center-periphery information sharing on several levels, including the failure of national organizations sharing information with local organizations, but also a failure by local

organizations to share information with national organizations. The author also considered the January 6 Capitol Hill Insurrection case, as well as the September 11th attacks on the World Trade Center and the Pentagon. These and other similar cases for further consideration in an expanded study are included at the end of this case study.

Introduction and Background: All was quiet in Alpharetta, Georgia on May 7, 2021. It was another sun-soaked Friday morning at the Colonial Pipeline headquarters, nestled in suburban office park thirty minutes north of Atlanta.[6] For decades, Colonial Pipeline operated inconspicuously, and that was the way CEO Joseph Blount liked it.[7] The first indications that something was wrong that morning emerged in the finance department, where analysts noticed an anomaly in the billing system. It appeared that malicious actors had broken in and were seizing customer information. Concerned that irregularities in the financial software would compromise the company's ability to accurately bill customers, the finance department quickly engaged Blount, who ordered the company to shut down the pipeline operations—effectively stopping the flow of a 5,500-mile system capable of moving three million barrels of oil per day.[8]

As Blount learned more details about the scope and scale of the hack emerged, he grew nervous. After a full day of frantic meetings, late on Friday evening, after speaking with cybersecurity experts who had previously dealt with the DarkSide hackers behind the operation, as well as with the FBI, Blount authorized a ransom payment of $4.4 million in exchange for a decryption tool that the hackers alleged would restore functions to the billing system.[9] In exchange for the ransom, the hackers gave Colonial Pipeline the decryption tool, which proved

[6] Weather provided by TimeAndDate.com; Directions and locations provided by Google Maps
[7] BBC, https://www.bbc.com/news/business-57178503
[8] NYT, https://www.nytimes.com/2021/05/10/business/colonial-pipeline-ransomware.html
[9] WSJ, https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

to be marginally useful. Leadership at Colonial Pipeline engaged a broader spectrum of U.S. federal agencies by Saturday morning, including the Cybersecurity and Infrastructure Security Agency (CISA), the agency nominally in charge of cooperating with all private sector companies and state- and local-partners. Why CISA had not previously engaged with Colonial Pipeline is unknown, but it is an open secret in the cybersecurity field that CISA is chronically underfunded and understaffed. Moreover, based in Washington D.C., they do not have offices or staff dedicated to regions or states, and are far removed from the day-to-day threats facing these U.S. private companies managing critical U.S. infrastructure.

Eventually, with the help of these U.S. agencies, Colonial Pipeline took a key server offline, effectively stopping the outgoing flow of information. But the damage was already done. The decision to shut down pipeline operations resulted in a disruption to the flow of oil on the East coast and panic buying at the gas pump up and down the eastern seaboard. Within days, more than half of the gas stations in Georgia, Atlanta, and South Carolina were without fuel.[10] Blount and Colonial Pipeline's predilection for anonymity would forever be destroyed.

Center-Periphery Information Sharing: The U.S. government is well aware of the use of cyber tools as a part of a broader set of emerging asymmetric tactics that global powers—especially Russia—are using to threaten foreign states and project power abroad. While it is still unclear whether the Russian government was ultimately behind the Colonial Pipeline hack, it's well known that as part of combatting and waging asymmetric warfare, Russia employs cyber tools as a nonmilitary offensive capability against a wide range of nonmilitary targets, including foreign governments, physical infrastructure, financial institutions, media outlets and in some

[10] Reuters, https://www.reuters.com/business/energy/top-us-fuel-pipeline-edges-toward-reopening-gasoline-shortages-worsen-2021-05-12/

cases, democratic elections.[11] Until recently, Russian nonmilitary offensive actions against democratic adversaries have been focused on targets in Russia's near abroad.[12] More recently, however, other countries have been hit by suspected Russian-sponsored cyber operations including the United States.[13]

Common features of these attacks are distributed denial of operations (DDoS), "worms" or malware attacks, and email hacks.[14] Cyber operations are often paired with disinformation campaigns from Kremlin-sponsored media outlets and automated bots and spam accounts on social media.[15] Vladimir Putin is said to favor cyber and disinformation operations because they offer a deniable way to deteriorate trust in Western democracy, especially elections.[16] Russia is not the only government targeting the United States using cyber tools. Other U.S. adversaries have directed attacks against U.S. critical infrastructure targets, including China, Iran, and North Korea.

The U.S. federal government has paid a lot of lip service to creating organizations and entire agencies devoted to understanding these issues, including several federal agencies tasked with identifying, responding to, and proactively defending against these threats. Signed under the Obama Administration, Presidential Policy Directive 41 (PPD-41) created a Cyber Unified Coordination Group and tasked the DOJ and FBI to take the lead on threat response activities through the National Cyber Investigative Joint Task Force (NCIJTF).[17] PPD-41 also tasked DHS

[11] Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11718
[12] The Atlantic, https://www.theatlantic.com/international/archive/2017/02/russia-disinformation-baltics/515301/
[13] National Public Radio, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[14] AP News, https://apnews.com/article/lithuania-coronavirus-pandemic-covid-19-pandemic-national-security-russia-4f643495296f645e8957594034ec0367
[15] Quartz, https://qz.com/1792155/russian-trolls-and-bots-are-successful-because-we-know-they-exist/
[16] Russia has also paired cyber operations with military and intelligence in combat and in the grey-zone, but this exceeds the scope of this paper.
[17] FBI, https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role

with serving as the lead agency for asset response activities through its Cyber Threat Intelligence Integration Center (CTIIC).

While DOJ and FBI are lead agencies for federal cyber threat response, DHS is tasked with coordinating with state, local, and private sector partners. One of DHS's mechanisms to carry out this coordination is the United States Cybersecurity and Infrastructure Security Agency (CISA),[18] which has a National Infrastructure Coordinating Center (NICC). The NICC coordinates and shares information about the nation's critical infrastructure, including providing situational awareness about threats, analyzing, and assessing emerging threats, providing recommendations to senior U.S. government leaders, and maintaining a network of on-the-ground partners, including the private sector. CISA's Infrastructure Security Division also operates a broad variety of critical infrastructure training programs, some of which allow for government officials, critical infrastructure owners including private sector companies, and interagency counterparts to learn about best practices.[19]

The United States also has offensive capabilities that can be used to deter adversaries' actions, or in response to an attack on U.S. infrastructure. In particular, the National Security Agency (NSA) and U.S. Cyber Command (USCYBERCOM) both have offensive capabilities. As of 2021, the Director of the NSA is "dual-hatted" as the commander of USCYBERCOM, which streamlines operational planning, deconflicting of activities, and coordination across the two organizations.[20]

Barriers to Information Sharing: However, while DoD, DHS, DOJ, and other bureaucracies have an important role to play in combatting the threat, each agency is hamstrung

[18] CISA.gov, https://www.cisa.gov/about-cisa
[19] CISA.gov, https://www.cisa.gov/critical-infrastructure-training
[20] Lawfare Blog, https://www.lawfareblog.com/ending-dual-hat-arrangement-nsa-and-cyber-command

by authorities and responsibilities to carry out defensive and offensive operations to deter or disrupt cyber threats. DoD can conduct intelligence and military operations overseas, but they lack significant authorities to operate domestically. DOJ and DHS are tasked with identifying and responding to domestic threats, but these national capabilities and tools at the center are a long way removed from state- and local-government partners at the periphery. This periphery includes private sector companies who oftentimes have more up-to-date threat information, including early warning on emerging attacks.

This case is an example of the national government bureaucracies failing to share information with local partners—or a failure of top-down center-periphery information sharing. In this case, it's clear that Colonial Pipeline did not have enough information about the hackers, which could have been easily provided by the U.S. federal government. Furthermore, federal agencies may have both lacked the legal authority to act, but it's more likely that they were unequipped to organize to respond, or to defense Colonial Pipeline against such an attack. Unarmed to defend against such a strong non-state actor, Colonial Pipeline leadership acted irrationally in a time of crisis, ultimately resulting in a small disaster for the energy sector on the East Coast.

Despite the nominal coordinating role that these federal agencies are required by law to play in the defense of U.S. infrastructure, the U.S. government currently lacks a point of contact in every state that allows for seamless coordination to defend infrastructure and election systems. As the case with Colonial Pipeline illustrated, the private sector had to move quickly, and while they allegedly spoke with advisors, which may have included U.S. federal officials, the company may have acted differently if they had access to a designated state-level task force dedicated to

cyber and infrastructure security. In this case, it's a lack of bureaucratic mechanisms to properly coordinate and defend.

Moreover, despite strong U.S. federal agencies and capabilities, without a unified and coordinated state-by-state model, the United States should expect to suffer from a disjointed state-by-state response to cyber-attacks on U.S. critical infrastructure and elections systems. The threats posed by cyber criminals span the globe and will only grow with time. Indeed, an independent dataset maintained by the Center for Strategic and International Studies (CSIS) documents over 700 global incidents since 2006.[21] Given the scope and scale of the threat, the United States has no choice besides rising to the challenge of defending public and private critical infrastructure and our democratic elections.

Conclusion: In this case, failure to share information from the center to the periphery takes place when the bureaucratic mechanisms proved insufficient to pass information. CISA and other government agencies simply are not set up to share information as widely as they should. Another reason that these organizations failed to share information from the center to the periphery is that there are simply too many organizations at the periphery. With hundreds if not thousands of U.S. private companies providing critical infrastructure services for the U.S. government, cyber defense organizations at the center cannot effectively share information with all the organizations at the periphery. In the case of the private infrastructure sector, this organizational constellation is complicated by the competing interests and resources of the federal U.S. government agencies, overlapping authorities, responsibilities, and conflicting policies. For information to flow properly from the center to the periphery, these roles need to be clarified, and clear guidelines for communication need to be established.

[21] Center for Strategic and International Studies, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Case Study #2: The Battle of Philippeville

Note: The author considered additional historical cases, including those of the United Kingdom colonial and the United States imperialist governments around the world. The author selected the French case because it was an example of information failing to flow from the peripheral local-level to the central national-level, in this case from the local sources of French military intelligence officers to the central French colonial system. It also has implications for center-periphery information sharing in the context of counterinsurgency campaigns.

Introduction and Background: Early in the morning on August 20, 1955, a mass of Algerians descended from the mountains into the town of Skikda. The eclectically armed group included farmers, industrial workers, and other local Algerians led by paramilitary forces from the armed wing Algeria's National Liberation Front (NLF), known as the National Liberation Army (ALN). As the armed mob closed in on Skikda, then known as Philippeville, members of the NLF who had been hiding out in cellars and basements around Philippeville popped out in a coordinated fashion, and began to open fire on the civilians, both Algerians and colonial Europeans.

The attack on Philippeville was the start of a series of ethnic riots across Algeria's Constantine region. These ethnic massacres in Philippeville triggered a swift and violent response by the French Army and French Algerian irregulars, marking a major escalation in violence between the French Army and the ALN, signaling a turning point in the Algerian War, and is remembered as one of the bloodiest conflicts in the war. The Algerian War, or the Algerian Revolution was a seven-year conflict between France and revolutionary elements in Algeria, primarily the FLN. Hostilities began on November 1, 1954. The Philippeville massacre,

also known as the Battle of Philippeville, took place in August 1955, and was one of the turning points for the war, signaling a shift from low level violence into all out conflict.

At the time of the Battle of Philippeville, the French officer in charge of intelligence collection and information sharing at Philippeville was a man by the name of Paul Aussaresses. Aussaresses began his career in French special operations and would eventually rise to the rank of General. Aussaresses served in WWII and later in Vietnam, and arrived in Algeria in 1955, where he was assigned to an intelligence unit in Philippeville. Aussaresses, in his new duty as an intelligence officer, was tasked with collecting information on emerging threats from the NLF and ALN using local Algerian sources ranging from business owners, local law enforcement, and others.[22] Aussaresses would eventually become infamous for his use of torture to gain information about impending attacks on French and Algerian military forces, but at the outset of his time in Algeria, he was primarily focused on gathering intelligence through human sources and methods.

As early as July 20, more than a month prior to the Philippeville attack, Aussaresses' sources started picking up signals that the town would be attacked.[23] An Arab grocer reported that he was selling flour at an exorbitant rate, indicating that guerillas were surrounding the town. The local police had reports that some 3,000 to 5,000 guerillas were in the mountains nearby, passing this information to Aussaresses who was quietly watching as information about the impending attack developed. Aussaresses would eventually learn the exact time and date of the attack from a pharmacist who was selling supplies to alleged guerrillas. More than a month in advance, Aussaresses had reams of information about the future battle, down to the hour.

[22] Brass, Martin. "Torture to Prevent Terrorism: Interview with Paul Aussaresses." Soldier of Fortune Magazine (2001).https://web.archive.org/web/20070212221901/http://www.military.com/NewContent/0,13190,SOF_0704_Torture,00.html
[23] Aussaresses (p.33)

Armed with this information, Aussaresses tried but failed to convince his superiors that the intelligence he had on the attack was good. His immediate commander, Lieutenant Colonel George Mayer, the commander of the 1st Parachute Chasseur Regiment, was skeptical, but sent Aussaresses to the regional commander, Colonel Decomps of the 2nd Bureau in Constantine. Decomps was downright dismissive, asking Aussaresses if there was any other intelligence about attacks on bigger cities like Constantine or Algiers. When Aussaresses said no, he was sent back to Philippeville to write a report. This report would be filed and sent to higher headquarters, noting the exact date and time of the August 20 attack. Nothing was done at the higher headquarters, and no reinforcements were sent to Philippeville.

At this point, Aussaresses was on his own, and realized that he alone would be responsible for preparing his men to defend against the impending attacks.[24] Aussaresses was careful not to tip off the NLF that he knew an attack was coming but prepared his men by positioning them throughout the city and putting his forces on alert across the villages in the region. Sure enough, on August 20, 1955, at 12:00pm local time, the NLF marched into Philippeville and began to open fire on the town's civilians. Aussaresses' forces were well prepared, and the NLF troops were allegedly high on "kif" a hashish substance, making them artificially brave, but under-performers in battle. The French garrison repelled the attack, losing only two troops, while the FLN lost more than 500.[25]

The towns around Philippeville were not so lucky. Nearby, the town of El Halia was stormed by a mob led by the FLN. More than 30 men, women, and children were brutally murdered in their homes. While Aussaresses was able to pre-warn the police forces in El Halia, they did not have the strength of numbers to defend against the NLF onslaught. After the NLF

[24] Aussaresses, Paul. "The Battle of the Casbah: Terrorism and Counterterrorism in Algeria 1955-1965." (2000)
[25] Aussaresses (p.52)

retreat in Philippeville, Aussaresses dispatched French infantrymen to El Halia, but they were too late. Several other towns were similarly targeted, the NLF indiscriminately killing civilians in an attempt to provoke the French colonial government into a harsh crackdown.

Indeed, the NLF's strategy paid off. The battle of Philippeville and surprise attacks in the surrounding areas resulted in a brutal crackdown by the French Army on the ALN and NLF, including the massacre of thousands of civilians. The long drawn-out war would be bloody and would quickly lose the support of the international community. Eventually, the failed French counterinsurgency would lead to the triumph of the ALN, NLF, and the independence of Algeria on July 5th, 1962.

Center-Periphery Information Sharing: At the time of the Battle of Philippeville, the French Army was split into divisions across Algeria. Aussaresses was in command of an intelligence unit, tasked with gathering information on the burgeoning revolution. Aussaresses' garrison was far enough from Algiers that it was on the periphery of the colonial system, but at the same time, it was much closer to the ALN and NLF strongholds, and therefore was receiving accurate information on the threat from the revolutionaries.

Traditionally, militaries are set up to provide information sharing mechanisms from the periphery to the center using the traditional military chain of command. This chain of command hierarchy also extends to non-military organizations, but in the case of the French military in Colonial Algeria, there was a clear line of command from Aussaresses, the ground commander on the periphery of the French military system, through his military superiors in Constantine, to the commander of all French forces in Algeria.

Aussaresses followed the standard policy for information sharing up the chain of command. He submitted an intelligence report, signed and endorsed by his boss, Colonel George

Mayer, which was then sent up the chain. However, one problem with the structure of the chain of command is that the perspective on information shifts as you go up the chain of command. While this can oftentimes be a benefit, in the case of Aussaresses, organizations at the periphery had information on impending threats, but this information did not match the perspective of the French military officers in Algiers at the higher levels of the chain of command.

Barriers to Information Sharing: At the time of the attack on Philippeville, French military officers and civilian officials in Algiers simply did not believe that the FLN existed. As soon as the FLN attack on Philippeville was launched, the French Deputy Prefect for the Philippeville region cabled Algiers in a panic, but no one acted on the report, just like they hadn't acted on Aussaresses report from two months prior.

In this case, it wasn't that information failed to be shared, but rather that the bureaucracy failed to act on information from the periphery. The perspective of the French Army intelligence collection at the periphery was at odds with the perspective of the French Army leadership at the center, and this disconnect resulted in a failure to provide reinforcements to Philippeville prior to the attack on the town.

Conclusion: The Philippeville case represents an instance where information from the periphery is passed to organizations at the center, but that information is never acted upon. This was a result of differing narratives at the periphery versus at the center. Aussaresses could see the threat on the ground at the periphery, but the French military officers at the center in Algiers were unable to see the situation on the ground, and therefore ignored the impending threats. The French civilian officials also had a role to play. French civilian leadership refused to believe that the NLF was real, because it didn't fit the narrative of a peaceful colonial occupation of Algeria. Indeed, there was no immediate threat to the French officials in Algeria, but they let this

preconceived notion color their judgement about the intelligence report with the exact date and time of the future attacks in Philippeville.

Extrapolating to other cases of information flowing from the periphery to the center, we can see that information sharing from the periphery to the center fails when the information from the periphery does not match the narrative or perspective at the center. While it's possible that information from the periphery oftentimes needs additional details to make it strategically relevant to organizations at the center, there are other times when information from the periphery is valuable on its own and must be acted on.

Other Cases for Consideration:

Other contemporary and historic cases in the United States illustrate bureaucratic mechanisms that prevent center-periphery information sharing on threats from domestic extremism, and transnational terrorism. The January 6, 2021, Capitol Insurrection and the September 11th, 2001, attacks on the World Trade Center and the Pentagon are contemporary examples that might make for good future cases that demonstrate how federal U.S. law enforcement agencies like the FBI, ATF, and others have failed to share information with local partners, thanks in part to bureaucratic failures.

During the Cold War period, the FBI monitored domestic extremist movements, including communist party members, white nationalists, and black power activists through its domestic counterintelligence program (COINTELPRO). The FBI paid informants in certain groups, including the KKK and Neo-Nazi parties, that informed the FBI in advance of certain attacks. However, information on these attacks was occasionally withheld from local government units, specifically state- and local-law enforcement. For example, prior to the Greensboro massacre in Greensboro, North Carolina, Bernard Butkovich, an undercover agent for the US

Bureau of Alcohol, Tobacco and Firearms (ATF), had infiltrated a unit of the American Nazi Party (ANP). When ANP and KKK members took part in the massacre, Butkovich knew that the attack was going to happen. During the 1985 civil trails following the massacre, Butkovich testified that he was aware that the KKK and ANP members intended to confront the demonstrators, but he did not tell the police or any other law enforcement agency. The Greensboro massacre also involved the FBI and Edward Dawson, a Klansman-turned FBI informant. Dawson was among the founders of the North Carolina Knights of the Ku Klux Klan when the North Carolina chapter of the United Klans of America split, and had been an FBI informant since 1969 under COINTELPRO. By 1979 he was also working as an informant for the Greensboro Police Department. He was given a copy of the march route by the police and informed them of the potential for violence. Nothing was done to stop the attack.

The FBI COINTELPRO case studies offer evidence to support a different argument, that organizations or bureaucracies may inhibit the flow of information from the center to the periphery in an attempt to save face. In this case, the FBI clearly did not want to publicize the fact that it was using KKK members as informants. In other cases, failure of information flow from the center to the periphery is inhibited by poor communication practices, as was the case with the January 6 Capitol Hill insurrection. All these cases are ripe for further study and would further contribute to the understanding of center-periphery information sharing.

SECTION VII: Implications and Conclusion

The two case studies and topics for further consideration all demonstrate failures of information flowing from the center to the periphery and vice versa. While this thesis project is limited in its scope, there are many other historical and contemporary examples of center-

periphery information sharing issues around the world. This thesis outlines some of the different ways that organizations can play a key role in center-periphery information sharing, but stops short of categorizing all the types of center-periphery information sharing challenges, which offers the promise of future studies on the topic.

As mentioned in the introduction of this paper, this study has four major relevant contributions to the study of political science and international relations. First, the study of center-periphery information sharing seeks contributes to the field of political science by expanding academic understanding of how power is given and distributed across the national and local levels of a nation-state. The concept of a nation-state can no longer be conceived exclusively as its national government alone. Power of states go beyond the federal executive, legislative, and judicial branches. Whether sharing information about cyber threats, transnational terrorism, or corporate espionage, the relationship between the center and the periphery illustrates the far-reaching impact on statecraft that events at the local level. This paper seeks to use this lens to demonstrate how other categories of power like military, diplomatic, and intelligence can also be projected across the center-periphery divide. Center-periphery information sharing failures help illustrate this theory, supporting the claim that power of a nation-state is generated at the local level—when information fails to flow from the local level to the national level, or vice versa, there may be grave consequences for national security and real implications for the power of a nation state.

Second, this paper shows that successful center-periphery information sharing is critical for assessing domestic vulnerability and threats within a nation state. This is even more important in an interconnected world where nation states are contending with unprecedented threats across the spectrum of national power. Failures of center-periphery information sharing

can result in mischaracterizing internal vulnerabilities like election systems, and critical infrastructure. Therefore, the concept of center-periphery information sharing has policy implications for understanding how governments apply national level information sharing resources to local problems, and how nations might apply some of the proven bureaucratic mechanisms developed for international information sharing and intragovernmental information sharing to better address gaps or blockages in center-periphery information sharing.

Third, the study of center-periphery information sharing is also relevant to how nation-states assess international and transnational threats. Failures of center-periphery information sharing can contribute to failures to stop catastrophic terrorist events like the Philippeville massacre. Moreover, as the Colonial Pipeline case shows, terrorism is not the only transnational threat states face in the 21st century. The failure of the U.S. government to protect Colonial Pipeline has important implications for the mismatch between cyber response and the inputs on transnational cyber threats and vulnerabilities not only across government agencies, but also across public and private sectors.

The final contribution of center-periphery information sharing is toward understanding how governments wage low intensity conflict, including counterinsurgency. Philippeville demonstrates how important local partners are (local leaders, intelligence sources, and informants) for COIN campaigns. For any successful information-based counterinsurgency strategy—indeed to address all national security threats nation states face in the 21st century—national powers at the center need to get information from the periphery at the local level (i.e., bottom-up), but national-level information also needs to flow from the center out to the periphery. By changing our conceptualization of the power of a nation-state to include the gaps and barriers to center-periphery information flow, we can hope to better address these threats.

SECTION VIII: Bibliography

Aussaresses, Paul. *The Battle of the Casbah: Terrorism and Counter-Terrorism in Algeria, 1955-1957*. (New York, Enigma Books, 2010).

Alilat, Farid. "Algeria: The dark side of French intelligence services during the war." TheAfricaReport.com (October 18, 2020).

Bardach, Eugene. *Getting agencies to work together: The practice and theory of managerial craftsmanship*. (Washington, D.C., Brookings Institution Press, 1998).

Bremer, Paul L., and Maurice Sonnenberg. *Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism.* (Pursuant to Public Law 277, 105th Congress, 1998).

Buckley, Chris, and Paul Mozur. "How China Uses High-Tech Surveillance to Subdue Minorities." NewYorkTimes.com (May 22, 2019).

Carnegie, Allison, and Austin Carson. *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation*. (Cambridge University Press, 2020).

Carson, Austin, and Keren Yarhi-Milo. "Covert Communication: The Intelligibility and Credibility of Signaling in Secret." *Security Studies 26.1 (2017):* 124-156.

Comfort, L. K., & Kapucu, N. (2006). "Inter-organizational coordination in extreme events: The world trade center attacks, September 11, 2001." *Natural Hazards*, 39(2), 309–327.

Cordner, G., & Scarborough, K. (2010). "Information sharing: Exploring the intersection of policing with national and military intelligence." *Homeland Security Affairs*, 6(1), 1–19.

Grauer, Yael. "Revealed: Massive Chinese Police Database. Millions of Leaked Police Files Detail Suffocating Surveillance of China's Uyghur Minority." *TheIntercept.com* (January 29, 2021)

Haider, Ziad. "The Attack in Kunming: Uyghurs and Beijing's Response." Truman Center.

Kean, Thomas H., and Lee H. Hamilton. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. (New York: Norton, 2004).

De Dreu, Carsten K.W. (2007), "Cooperative Outcome Interdependence, Task Reflexivity, and Team Effectiveness: A Motivated Information Processing Perspective", *Journal of Applied Psychology*

Jervis, Robert. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. (Cornell University Press, 2010).

Kurup, Rohini, and Wittes, Benjamin. (2021) "Was Jan. 6 an Intelligence Failure, a Police Failure or Both?" *Lawfare Blog.*

Lambert, D. (2018). "Addressing challenges to homeland security information sharing in American policing: Using Kotter's leading change model." *Criminal Justice Policy Review*.

McDermott, Rose, and Uri Bar-Joseph. *Intelligence Successes and Failure: The Human Factor.* (Oxford University Press, 2017)

McManus, R. W., & Yarhi-Milo, K. (2017). "The Logic Of 'Offstage' Signaling: Domestic Politics, Regime Type, And Major Power-Protégé Relations." *International Organization, 71(4),* 701-733.

Middlemiss, A., & Gupta, N. (2007). US interagency law enforcement cooperation since September 11, 2001: Improvements and results. *Journal of Financial Crime, 14*(2), 138–149.

Nouzille, Vincent. *Les tueurs de la République: assassinats et opérations spéciales des services secrets (The Killers of the Republic: Assassinations and Special Operations of the French Secret Services).* (J'ai Lu, 2016).

Andrew, Christopher, Richard J. Aldrich, and Wesley K. Wark. *Secret Intelligence: A Reader*, (New York, London, Routledge, 2009).

Strom, Kevin J., Hollywood, John S., Pope, Mark. (2015) "Terrorist Plots Against the United States: What We Have Really Faced, and How We Might Best Defend Against It" *RAND Corporation.*

Sedgwick, D., & Hawdon, J. (2019) "Interagency Cooperation in the Era of Homeland Policing: Are Agencies Answering the Call?" *American Journal of Criminal Justice* 44**,** 167–190.

Senate Select Committee, *Book III: Supplementary Detailed Staff Reports*, 94th Cong., 2d sess., 1976, S. Rep. 94–755.

Zegart, Amy. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. (Princeton University Press, 2007).