Covert Sources of Digital Economic Backwardness

How Foreign Threats Can Cause States To Limit Access to Technology; a Formal Argument

by

Joel D. Watson

Advisor: Professor Michael Joseph

A Senior Honors Thesis Sumbitted to the
Department of Political Science,
University of California, San Diego

March 29, 2024

Acknowledgements

Thank you to my inspiring thesis advisor, Professor Michael Joseph. Professor Joseph challenged me to take my inkling of a research question, get excited about its implications, and carry it into new directions; now, I am more interested than ever in this field. His guidance, within and outside of my project, has been valuable and encouraging, and my progress was made possible by his flexibility and support throughout the process. I look forward to using Professor Joseph's brilliant insights in my research and writing from now on, and I thank him for making this project one of my favorite experiences.

Thank you to Professor Scott Desposato and Professor Sean Ingham, who made a great team leading our Honors Seminar. I deeply appreciate their personal and professional advice, and felt very comfortable working with them and participating in their class. They, along with our amazing TAs, Anthony Anderson and Linh Le, have been role models for us in the seminar, and all went out of their way to give us their time, resources, and encouragement. I thank them all for their admirable dedication and commitment.

Thank you to all the students in the seminar, for the important feedback and encouragement on my project. I thank them additionally for giving me the opportunity to learn about their theses and academic interests; the Honors Seminar was also a key social outlet for me, and I always looked forward to catching up with the other students in class.

Finally, thank you to the professors, instructors, and advisors who introduced me to the Honors Seminar. Thank you to my dad, for encouraging me to do an honors thesis and go further in school, and my mom, and my sister, for supporting me in all my extracurricular activities at the same time.

Covert Sources of Digital Economic Backwardness

How Foreign Threats Can Cause States To Limit Access to Technology; a Formal Argument

A Senior Honors Thesis Sumbitted to the

Department of Political Science,

University of California, San Diego

March 29, 2024

Contents

1 Introduction

Internet and communication technologies (ICTs) have had a transformative, welfare-enhancing effect on the modern world. Especially with the rise of the Internet, these technologies enhance innovation, reduce transaction costs for firms, and boost the provision of public services, among other benefits.

Scholars of international conflict have identified important effects of ICTs for that field, too. For one, ICTs can improve war-fighting capabilities by facilitating military organization and coordination, and may give the public a louder voice in conflicts (Feldstein, 2022). ICTs are also vital for preventing and deterring secretive attacks, by improving monitoring and exposing covert operations (Joseph and Poznansky, 2018). The latter effect is critical to modern conflicts, because powerful states rarely use overt force against their adversaries. Instead, they use "grey-zone" tactics, cyber attacks, or election meddling to achieve their foreign policy goals (Kapusta, 2015). Thus, the targets of these attacks face strong incentives to encourage investment into ICTs (in addition to the economic/welfare incentives).

However, our observations don't always match this intuitive expectation. In critical cases, regimes facing foreign threats still deny their citizens access to critical ICTs (Freedom House, 2023), limiting their economy and capacity to respond to covert operations. What is more, these are often cases where more ICTs are desperately needed.

Why do regimes deny access to ICTs? One explanation is that they fear that technologies like ICTs will help the public revolt against them and produce unrest (Acemoglu and Robinson, 2006). But this domestic explanation is unlikely the whole story, especially in the context of modern ICTs.

For instance, countries like Iran, Russia, Kenya, and Nigeria all have similarly high levels of domestic instability ("Fragile States Index", 2023). However, Iran and Russia have been bigger targets of foreign covert intervention by powerful adversaries like the United States (Arkin et al., 2019; Graphika, 2022; Sanger, 2012; Lake, 2016). We might expect that these foreign threats would cause those countries to invest more in ICT access. However, we see the opposite: even though Iran and Russia face larger foreign threats, they block access to ICTs more than Kenya and Nigeria (Freedom House, 2023). Moreover, some countries, including democratic states, are more domestically stable, yet still take steps to restrict ICTs (Freedom House, 2023).

I offer a theory to address these issues. First, I use a formal model to argue that foreign threats–specifically, covert threats–can create, rather than counteract, incentives to block ICT access. I show that, in most cases, foreign threats do encourage states to invest in ICTs, to better thwart covert operations. However, when investment in ICTs would encourage a covert intervener to instead attack overtly (which is more costly), the threatened state may instead block ICT investment and tolerate covert intervention. I use the term ”underinvestment” to refer to this result–when a state blocks citizens' access to ICTs with the purpose of limiting a security threat.[1]

This novel explanation suggests that technological underinvestment (i.e. blocking ICTs) can occur under conditions that have not yet been formalized. It also contributes to our understanding of the concept of economic backwardness–when a state deliberately blocks access to technology that would have induced economic growth and improved welfare. Specifically, my prediction illustrates a case in which economic backwardness is caused solely by foreign threats. This is interesting, because existing theory expects only domestic threats to produce backwardness (Acemoglu and Robinson, 2006).

Second, I develop an extended model that integrates both domestic and international threats to consider their implications for ICT access. This model is specifically designed to illustrate ICTs and modern conflict, because it assumes that covert operations work via the digital world, often using ICTs to influence domestic politics in favor of a foreign intervener (Stout, 2017). (A prominent example of covert influence is Russian election meddling via social media (Young, 2020)). Thus, the model assumes that, while they still increase the risk of covert exposure, modern ICTs may also help interveners conduct covert action more effectively (e.g. more social media access means online election meddlers can influence more people).

With this model I make several interesting findings that integrate international and domestic theories of technology access and conflict, and refine the standard logic of domestically-induced underinvestment in ICTs.

First, by including the domestic population, my model generates predictions for underinvest-

[1] I use the terms underinvestment and blocking somewhat interchangeably to describe a state's choice to deny citizens access to new ICTs. Debs and Monteiro, 2013 and other scholars of international relations use the former, which implies that the government is involved in investing and creating new technological innovations. Acemoglu and Robinson, 2006 and other scholars of economic backwardness use the latter, which depicts states banning existing technologies from being accessible in their marketplace. My theory applies to both kinds of choices, since each can limit technologies that would otherwise improve welfare and affect the detection of covert operations.

ment that are robust to the current understanding of economic backwardness, where a state blocks technologies that would facilitate domestic unrest and threaten elites' power (Acemoglu and Robinson, 2006). The model also shows that foreign threats usually encourage ICT investment, another expectation of existing theory.

Second, under conditions where domestic threats would not cause a state to block ICTs, the model predicts that international threats *can* induce blocking, through two different pathways. Thus, my theory expands the conditions under which we should see underinvestment, potentially explaining a mismatch between Acemoglu and Robinson and certain empirical analyses.

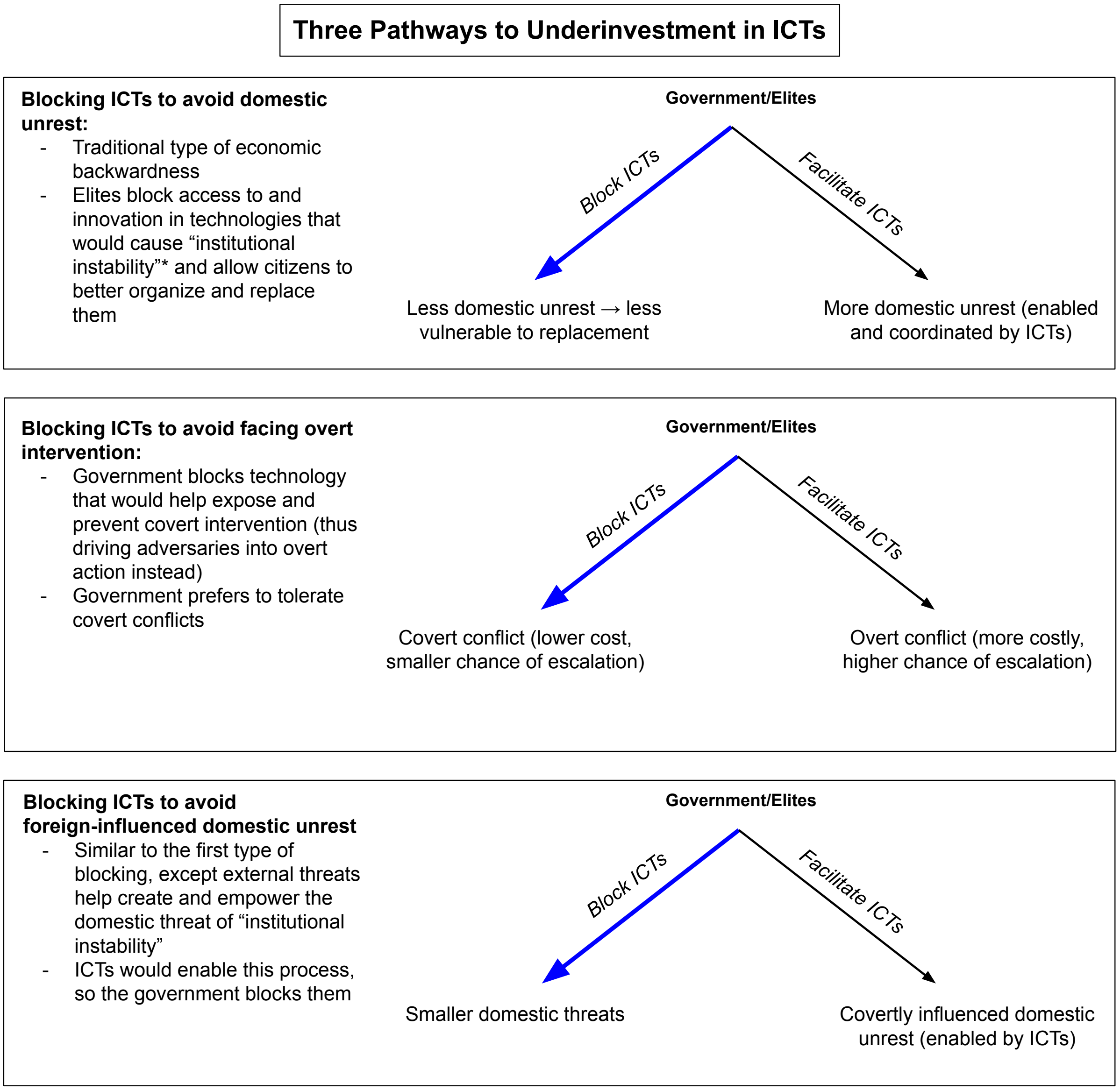
The first of these is a result similar to my initial novel prediction–that the fear of foreign overt intervention can cause states to block ICT investments, allowing them to instead face covert intervention but causing technological backwardness.

Additionally, the extended model illustrates a new hybrid dynamic where domestic and foreign threats interact, through covert influence, resulting in underinvestment in ICTs. In this interaction, foreign covert operations use ICTs to manipulate public opinion against a target government. Concerned that investing in ICTs could improve covert influence, increasing domestic unrest, the target state blocks investment to avoid that outcome. This prediction is similar to existing backwardness theory, in that the state underinvests in technology to avoid domestic unrest. However, the unrest in this new mechanism is actually incited by foreign covert intervention. Thus, this novel prediction also modifies our existing understanding of economic backwardness, by providing another avenue by which external threats induce technological underinvestment.

Finally, I use the model to study Iran's ICT policies over the last two decades. Iran is a relevant case because (1) it worries about covert intervention from foreign rivals, and (2) while the regime is popular among some groups, there is considerable dissatisfaction, especially in urban centers and among youths (Ranalli, 2022). Indeed, Iran has often claimed that the United States stokes domestic revolt through covert meddling (Rhoads and Fassihi, 2011). Iran's ICT policies are also nuanced: in some cases, the government blocks ICT access, limiting economic productivity and welfare; in other cases, it encourages access. I argue that my hybrid blocking mechanism explains their ICT policies, given the complementary combination of international and domestic threats.

This paper contributes to existing literature by connecting our understanding of foreign intervention to the domestic economic backwardness literature, proposing conditions under which foreign threats can lead to underinvestment in ICTs. This adds nuance to Acemoglu and Robinson's domestic politics-focused theory, which argued that external threats only discourage backwardness.

My theoretical predictions could also guide empirical research. The first novel result–underinvestment caused solely by foreign threats–provides a possible explanation for observations of economic backwardness that cannot be explained by the existing domestic mechanism. The second novel result–underinvestment as a result of domestic and foreign threats through covert influence–speaks to the need to study modern economic backwardness as a function of both domestic and international factors. And unlike existing theories of backwardness, my model predicts that these mechanisms for underinvestment can occur in democracies, offering a possible explanation for recent steps that democratic governments have taken (including the U.S.) to limit foreign online influence.


Three Pathways to Underinvestment in ICTs

Blocking ICTs to avoid domestic unrest:
- Traditional type of economic backwardness
- Elites block access to and innovation in technologies that would cause "institutional instability"* and allow citizens to better organize and replace them

Government/Elites
Block ICTs
Facilitate ICTs
Less domestic unrest → less vulnerable to replacement
More domestic unrest (enabled and coordinated by ICTs)

Blocking ICTs to avoid facing overt intervention:
- Government blocks technology that would help expose and prevent covert intervention (thus driving adversaries into overt action instead)
- Government prefers to tolerate covert conflicts

Government/Elites
Block ICTs
Facilitate ICTs
Covert conflict (lower cost, smaller chance of escalation)
Overt conflict (more costly, higher chance of escalation)

Blocking ICTs to avoid foreign-influenced domestic unrest
- Similar to the first type of blocking, except external threats help create and empower the domestic threat of "institutional instability"
- ICTs would enable this process, so the government blocks them

* From Acemoglu and Robinson (2006): *Economic Backwardness in Political Perspective*

Figure 1: Theoretical Predictions

2 Concepts

This paper focuses on media technologies and the extent to which governments invest in them. I refer to media technologies as ICTs (Information and Communication Technologies), a term to describe technologies that collect and share information and the systems of communication in which they operate (OECD, n.d.-a, CSRC, n.d.). A prominent effect of ICTs is that they enhance coordination among actors within and among communities (Shirky, 2008; Diamond, 2010). ICTs thus include newspapers and the media, radios, and television, as well as “media awareness” factors like school enrollment and international media access (Joseph and Poznansky, 2018). I also include the Internet and social media platforms as ICTs, because access to these systems heavily impacts coordination on small and large scales (Bertot et al., 2012; Stein, 2017).

Since this paper focuses on international relations and national security, it is important to highlight why ICTs differ from other innovations that impact security. On one hand, innovations in weaponry and defensive devices help fight wars with physical force. So, the main effect of these innovations is a shift in the capacity to win wars directly (Debs and Monteiro, 2013).

On the other hand, the role of ICTs as they relate to conflict between and within states, primarily comprises rapid communication, monitoring adversaries, gathering intelligence, and coordinating secretive groups (Arena and Wolford, 2012). Thus, the main security effect of ICT innovations is on the ability to conduct military actions in secret. Specifically, ICTs may limit this ability by helping governments identify secret attempts to harm them by foreign or domestic forces (Joseph and Poznansky, 2018). But in certain cases, ICTs can help violent groups organize more effectively (Dragu and Lupu, 2021). In either case, the influence of ICTs comes from their capacity to identify and monitor and to facilitate communication.

Investment in ICTs refers to the extent to which governments facilitate their citizens’ access to technology, connect media institutions to them, and enable technological innovation. “Innovation” can refer to both the domestic invention and improvement of new technologies or the importation of technologies developed elsewhere, both of which contribute to industrialization and economic development (Gerschenkron, 2014). Conceptually, the amount by which a government encourages ICT access and innovation can vary. On one side of the scale, a government might place no restrictions on media access and would readily fund research that could produce innovations. At the other extreme, a government might ban Internet access and the sale of technology, and restrict imports of ICT products.

These extreme examples of investment and non-investment are historically rare. Instead, there is much variation in the extent to which governments facilitate ICT access and promote innovation. However, at the individual policy level, the difference between “restricting” and “encouraging” ICTs is more discrete. Governments make regulatory choices, like raising or lowering taxes on products and levying tariffs on imports. They may also subsidize certain industries or give contracts to technology companies. They may even ban or promote a specific device or media platform. These distinct choices are what my model illustrates (in the form of a government's investment decision).

Overall, scholars agree that ICTs improve economic productivity. Thus, holding security concerns constant, blocking ICTs decreases welfare by limiting citizens' access to modern technologies that reduce transaction costs, improve communication, and even increase leaders' own income and popularity. These benefits suggest that governments should make decisions which resemble the very facilitative side of the ICT investment scale.

However, theoretical and empirical research also frequently studies the effects technologies like ICTs have on welfare, conflicts, organization, and communication. From these effects, scholars have identified (informally and formally) several factors that can incentivize governments to encourage or restrict ICT access for their citizens. There are two separate literatures that explore the effects of ICTs on security concerns.

2.0.1 The Foreign Threat Literature

One literature studies how ICTs help states guard against the threat of foreign influence by improving their ability to monitor and detect covert actions, or grey-zone conflicts. Scholars in this area use important historical and modern cases to suggest that since ICTs improve monitoring, they allow states to better detect and prevent covert actions against them. Intuitively, this literature suggests that international threats have the same effect as economic incentives on technological innovation. However, this logic has not been studied formally, so it lacks a clear theoretical picture of how ICTs impact the incentives for conductors of covert intervention, and predictions about this relationship's effect on a state's ICT investment.

Covert intervention is primarily seen as an attractive alternative to overt force because concealing one's activities can allow a state to maintain plausible deniability of its involvement in foreign events. This may allow leaders to conduct operations whose goals may be unpopular among citizens, without facing criticism (Baum, 2004). Keeping operations secret can also avoid public fallout should they fail (Joseph and Poznansky, 2018). Conflicting states may also try to keep their confrontations secret to prevent escalation to widespread violence or an overt war (Carson, 2016), and historical evidence suggests that leaders purposely avoid exposing covert intervention for this purpose (Carson, 2018). And more broadly, covert action seeks to accomplish a policy goal while avoiding the vast physical costs of overt action. Due to its limited scale, though, covert intervention is usually less likely to succeed (Levin, 2016; Joseph and Poznansky, 2018).

However, many of these additional benefits are largely conditional on the covert action remaining undetected. Joseph and Poznansky, 2018 argue, "a leader's primary rationale for choosing covert action is the promise of plausible deniability," which becomes harder as the chances of exposure increase (4; Lowenthal, 2023, 231). The likelihood of being detected is a key factor impacting the expected benefits, costs, and risks of covert action. Once they are harder to conduct undetected, covert activities become less appealing to policymakers.

Since ICTs facilitate coordination among domestic actors, they improve the ability of states to detect and expose evidence of foreign covert actions against them. This suggests that foreign adversaries would prefer to covertly intervene against states with fewer ICT capabilities, to ensure the maintenance of plausible deniability. By the same logic, as ICT levels increase, we should expect foreign interveners to prefer to conduct no intervention (or strictly diplomatic maneuvers) or take overt actions rather than covert operations.

Joseph and Poznansky test this expectation using research from Warren, 2014 (including Banks Dataset and World Bank data) which measures the level of different ICTs, including radio, television, telephone, and newspapers, in various countries over time (Joseph and Poznansky, 2018). They take instances of covert intervention by the United States from Downes and O'Rourke, 2016 and Levin, 2016, and, along with the data measuring ICT levels, determine that "the USA is consistently less likely to pursue covert action relative to both no intervention and overt action as the potential target's level of ICTs increases" (321). Joseph and Poznansky argue that "access to communications and media technologies across all states increases over time, yet the targets of covert interventions consistently have low access" (328).

While ICTs do increase the likelihood of covert exposure, interveners may also employ a target state's ICTs to secretly influence populations during a covert intervention. During the Cold War, many covert operations run by the United States relied on ICTs to spread information, coordinate groups, and sway public opinion in support of policy goals (Cormac et al., 2022; Doyle and Kornbluh, 2017; Johnson, 2021(23); Valdivia, 1991). Often, these goals entailed overthrowing or voting out a government. More recently, actors have used contemporary ICTs for similar purposes. Notably, Russia has used social media to spread misinformation and conduct election interference

(Badawy et al., 2018; Stelzenmüller, 2017; Wilde and Sherman, 2022). This kind of online influence may not be strictly covert, too; simply having access to foreign media platforms could help spread ideas that align with a foreign intervener's goals. Additionally, many states use or sponsor cyberattacks, which take advantage of technological systems to infiltrate foreign institutions and disrupt military, financial, and government activities; such operations occur frequently and may also serve to avoid overt escalation (CFR Cyber Operations Tracker, n.d.; Carson, 2018).

Although this existing literature empirically covers the effects of ICTs on how states conduct foreign intervention, the subject remains theoretically underexplored. Further, research has yet to study how the effect of ICTs on foreign intervention impacts the extent to which governments invest in them. Intuitively, though, we might expect that the threat of covert intervention would encourage states, particularly geopolitically vulnerable ones, to support media access and encourage innovation, to make covert intervention against them more difficult. [2]

2.0.2 The Domestic Unrest Literature

Another literature argues that ICTs and other innovations affect domestic threats of rebellion, making leaders concerned about being replaced. Specifically, some governments may expect technological change to threaten their power, by "erod[ing] their political advantages" or decreasing the public's cost of replacing them (Acemoglu and Robinson, 2006). For instance, by improving coordination, ICTs may encourage citizens to protest government policies, and help organize revolts (Yang, 2013; Gainous et al., 2015; Castells, 2015). Acemoglu and Robinson, 2006 use a game-theoretic model to show that in cases when innovations would make them more vulnerable to replacement by their citizens, political elites may "block" technological innovations. Their model reflects how:

> ...all else equal, the elites prefer technological change. All else is not equal, however, because such change may erode their political advantages relative to other groups that are benefiting from the changes or weaken their ability to control political challenges. As a result, in certain circumstances, institutional and technological change will increase the likelihood that the elites will lose power, creating the political replacement effect.

[2] Acemoglu and Robinson, 2006 argue that external threats always encourage elites to invest more in technology. However, they do not specify the different types of external threats that states might face.

(2006, 116).

Thus, their model illustrates how the threat of replacement by the domestic public, under certain conditions, may encourage elites to block innovations in technology and industry. Since we would otherwise expect governments to allow technological innovations given the economic benefits, blocking such innovations is called "economic backwardness." Before Acemoglu and Robinson, this concept was studied by Alexander Gerschenkron, who observed that in many countries exhibiting backwardness, "the State clearly became an obstacle to the economic development of the country" (Gershenkron, 1970: 89, quoted in Acemoglu and Robinson, 2006).

Acemoglu and Robinson's model is a compelling theoretical argument for domestically induced economic backwardness. They apply their model by comparing the adoption of new technologies in several countries during the Industrial Revolution, confirming that rulers who were more vulnerable to replacement blocked industrialization (125). Some subsequent empirical research studying recent cases supports this theory (Leonida et al., 2013). Other scholars, however, question its empirical applicability (Dragu and Lupu, 2021). Additionally, it remains uncertain whether newer ICTs, like social media and digital technologies, actually assist the public in collective action against repressive regimes, or whether they give authoritarian governments more tools to apply repression; current research points in both directions (Diamond, 2010; Dragu and Lupu, 2021; Farrell, 2012; Feldstein, 2021; Tucker et al., 2017). In my extended model, the parameter relationships reflect the assumption that ICT innovations may reduce the cost of revolting, but by how much depends on modifiable parameter values.

This paper suggests that the assumptions these two literatures make about ICTs, external threats, and backwardness are insufficient. I aim to draw a formal picture of the logic of foreign intervention (including an intervener's consideration of how ICTs might expose covert intervention and their alternative methods for intervention), and how awareness of this logic influences a target state's approach to ICTs. I will argue that, while we can usually expect foreign threats to encourage ICT investment, some states may prefer to restrict ICTs and tolerate covert intervention, if expanding ICT access would render covert actions too vulnerable to exposure and drive an intervener to instead use overt action.

To do this, I use a game-theoretic model. This allows me to consider the individual incentives of actors (i.e. the target state and the intervener) and quantify the costs, benefits, and risks of relevant factors. With these tools, I make predictions about when a state might invest or underinvest in ICTs, and the conditions that produce each result.

I then extend the model to study the effect of ICTs on a particular type of covert intervention–covert influence. This allows me to incorporate the domestic incentives for ICT investment with the foreign intervention threat incentives. The extended model yields conditions under which states block ICT investment due to domestic concerns, foreign intervention concerns, and the concern of covertly influenced domestic unrest (a combined foreign and domestic concern). Interestingly, when the model's parameters are set such that it illustrates a democracy before an election, the model predicts that blocking can only occur when a foreign threat is present (either the threat of overt intervention or a covertly influenced replacement if ICTs become more accessible), and not when there is potential domestic unrest only. Finally, I study Iran's ICT restrictions as a case study of blocking due to the concern of covertly influenced domestic unrest.

3 Model

In this section, I construct an initial model of two competing states, one which decides whether to invest in its ICT capabilities (the "investment" decision) and the other which decides whether and how to intervene against the first state, given the level of technological innovation and access in the first state and the effects of that technology on covert action. The intervening state's decision represents the informal intuition developed by Joseph and Poznansky, 2018 and others.

I highlight the equilibrium in which the first state (the Target state) blocks ICTs (a.k.a. underinvests). I also illustrate the effects of the model's parameters on which equilibria are reached.

This model is important because the effect of international threats on domestic ICT investments has not been modeled before. My model formalizes this relationship, and illustrates an interesting prediction: the fear of international threats can produce underinvestment in ICTs–a type of economic backwardness. Specifically, when a target state fears that improving its ICTs will lead to overt intervention against it (by making covert action more vulnerable to exposure for adversaries), the target state may rather block ICT investments to instead face covert intervention.

3.1 Model: The Effect of International Threats on ICT Investments

In this model, there are two players: the target state (T) and the intervening state (A, for Adversary). Specifically, these players represent the governments or leaders of each state (not their populations as a whole). As is common in the covert conflict literature on which I build, I emphasize a setting where A is powerful and can intervene against and overthrow T using covert or overt force.

I assume that A wants to overthrow T, while T wants to stay in power. This is a complete information model, and I solve for sub-game perfect equilibria in pure strategies. The sequence of moves and payoffs are shown in Figure 1.

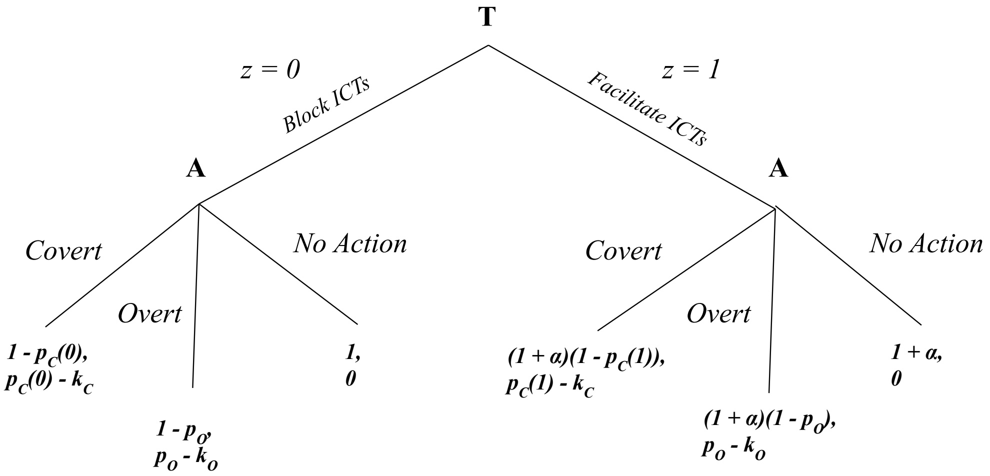


Figure 2: Baseline Model Game Tree

Parameter	Interpretation
$\alpha > 0$	The benefit T gets from investing in ICTs.
$p_C(z) \in (0,1)$	The probablility that covert action succeeds as a function of z (ICT investment)
k_C	The cost of covert action for the Intervener (A)
$p_O \in (0,1)$	The probability that overt action succeeds
k_O	The cost of overt action for A

Assumption	Interpretation
$p_C(0) > p_C(1)$	Innovating lowers the probability that covert action succeeds (by making it more vulnerable to exposure)
$p_O > p_C(z)$ for all z	Overt action is more likely to succeed than covert action[3]
$k_O > k_C$	Overt action is more costly than covert action

Formally, a strategy profile for T is $s^T(z \in \{0,1\})$, where $z = 1 \implies T$ facilitated ICTs. A strategy profile for A is $s^A(a \in \{Covert,\ Overt,\ No\ Action\}|z)$. This notation will be used in formal proofs in the Appendix.

Covert and Overt intervention are costly lotteries that determine whether A succeeds with probability p_C and p_O, respectively. Facilitating ICTs lowers p_C, raising the probability that covert intervention fails by being exposed. However, facilitating ICTs has no effect on the lottery for overt

[3] This assumption is based on the limited scale and lower probability of success of covert intervention compared to overt intervention, which is larger scale and uses more force (Levin, 2016; Joseph and Poznansky, 2018)

intervention (p_O).

This highlights the substantive characteristics of each type of intervention and their relationship with ICTs. The key challenge of covert action is to sustain secrecy. The main use of ICTs (in this paper) is for monitoring, detection, and communication, all which endanger secrecy, reducing the success of covert action. Since secrecy is not a major component of overt operations, their success is not impacted in the same way.[4] Thus, the model assumes that ICTs affect p_C but not p_O.

3.1.1 How to Interpret the Investment Decision

An important feature of the model is that T benefits from facilitating, or investing in, ICTs. Consistent with my substantive motivation, I assume that investment in ICTs has a positive economic impact, and therefore would raise the tax base that T could take from, and improve their own approval. I capture this with variable α. Correspondingly, if T stays in office after investing, its overall payoff is larger than if it hadn't invested. Also, to put a higher burden on finding backwardness, I assume that T pays no extra costs for facilitating ICTs.

Underpinning these assumptions is the overall belief that ICTs enhance welfare, and as a result, we can define the choice to block ICTs as inefficient because the economy will perform worse. Thus, we can substantively define underinvestment as follows:

Definition (Underinvestment): In any equilibrium in which T blocks ICTs (i.e. when T plays $z = 0$), I say that T underinvests in ICTs. In any equilibrium where T facilitates ICTs (i.e. plays $z = 1$), T is said to invest. [5]

I think the investment decision is an accurate representation of a scenario that states often face. As mentioned in Concepts, it is rarely the case that leaders outright deny or freely provide ICTs to their citizens, but they do face choices where they could expand or limit these economically efficient investments. I characterize underinvestment as a case where the state chooses to limit this kind of investment at a particular moment, or for a particular aspect of ICTs.

[4] Any effects of ICTs on war-fighting capability would be felt in both overt and covert action, so I do not model them.

[5] See footnote 1

3.2 Results and Analysis

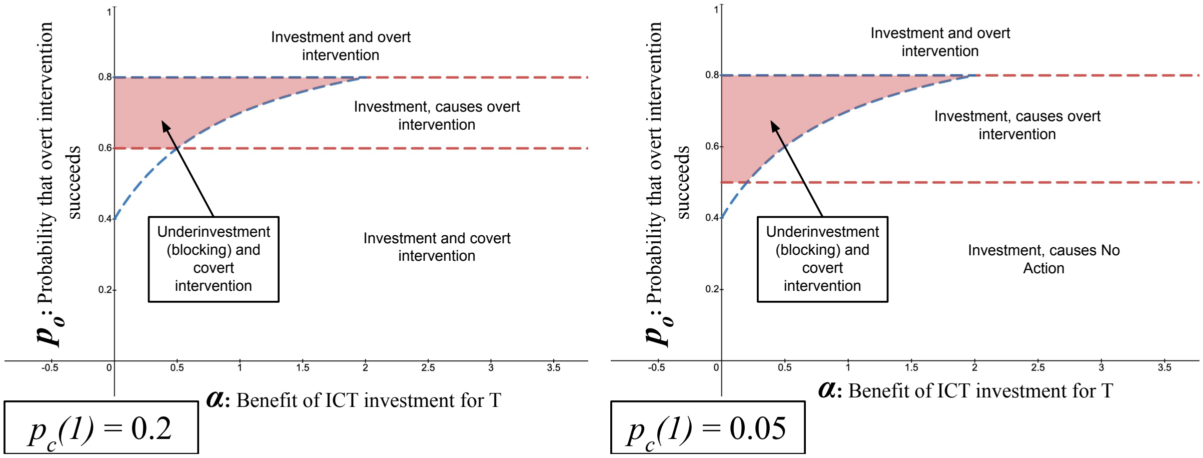


Figure 3: Equilibria as a function of α and p_O

Notes: Assumes $k_O = 0.5, p_C(0) = 0.4, k_C = 0.1$.

Equilibrium	On-path Actions	Off-path actions (A's preferences)
Underinvestment (blocking) and Covert Intervention	T blocks ICTs and A conducts Covert intervention	A would conduct Overt intervention if T facilitated ICTs
Investment, causes Overt Intervention	T facilitates ICTs and A conducts Overt intervention	A would conduct Covert intervention if T blocked ICTs
Investment, Overt Intervention	T facilitates ICTs, and A conducts Overt intervention	A would conduct Overt intervention regardless of ICT levels
Investment, Covert Intervention	T facilitates ICTs, and A conducts Covert intervention	A would conduct Covert intervention regardless of ICT levels
Investment, No Action (not pictured)	T facilitates ICTs, and A conducts No Action	A would conduct No Action regardless of ICT levels
Investment, causes No Action	T facilitates ICTs, and A conducts No Action	A would conduct Covert intervention if T blocked ICTs

Figure 3 plots equilibria as a function of p_O and α. All the model's equilibria are described in the table.

Intuitive scholars have explored the anticipatory effects of international intervention on the decision of whether to invest in ICTs. They typically find that as the threat of overt intervention increases, states are more likely to invest in ICTs to guarantee that they can detect covert intervention and raise the probability that they will deter overt intervention (Joseph and Poznansky, 2018). I rationalize these as equilibria in the model; however, they are not the whole story.

As the plot and table show, many equilibria commonly rationalized by past scholars (in white) are realized in the model. For example, when the benefit of ICTs is high enough, T always facilitates them. When T is only threatened by covert intervention (left plot, $p_O < 0.6$), T invests in ICTs to have a higher chance of exposing covert operations.

Highlighted in red is the underinvestment equilibrium, a new strategic outcome. Here, we see that the fear of overt intervention can cause T to block ICTs. Because this is novel, I characterize its features below.

Proposition 3.1 ***Underinvestment Equilibrium:*** *If $p_C(0) - k_C \geq p_O - k_O \geq 0, p_C(1) - k_C$ and $1 - p_C(0) \geq (1 + \alpha)(1 - p_O)$ are satisfied then the following strategies are sub-game perfect. T blocks ICTs. A selects Covert intervention if T blocked, and Overt intervention if T facilitated. On the path, we observe underinvestment in ICTs, which induces Covert intervention.*

Remark (The threat of overt intervention drives underinvestment in ICTs): If A's threat of Overt action was non-serious ($p_O - k_O < 0$), then T would facilitate, not block, ICTs. After this, A would not overtly intervene because No Action has a higher payoff.

Proposition 3.1 is proven in A.1.1. The logic of the equilibrium is as follows.

Under the conditions of 3.1, A's best choice is covert intervention when T does not invest in ICTs. If T does invest in ICTs, the risk of exposing A's covert actions rises so much that covert intervention is no longer viable. A would then turn to its second-best option, overt intervention.

So from T's perspective, investing in better ICTs pushes A from covert operations that have a reasonable chance of failing (outright or by exposure), to an overt intervention, which is more costly and likely to depose T. T does not like the threat of covert intervention, but prefers to live in a world where they occur, rather than force A's hand into taking overt actions–which is much more threatening to T.

This insight is theoretically and substantively important. Theoretically, the existing covert intervention literature already shows that ICTs reduce the risk of covert intervention (Joseph and Poznansky, 2018). However, by implying that Targets should prefer more ICTs, it fails to consider the Intervener's (A's) strategic incentives. This common implication only follows if the A's next best alternative is no intervention altogether, not overt intervention.

Substantively, countries like North Korea and Venezuela have the United States as a powerful adversary, and they often accuse the US of meddling in their affairs (Cohen, 2018; "U.S. Relations With the Democratic People's Republic of Korea", 2021; "U.S. Relations With Venezuela", 2023; Associated Press, 2010; Lansberg-Rodriguez, 2015). The US has taken actions to influence politics in both countries, and has considered overtly intervening in the latter case (King, 2019; Goodman and Mustian, 2024; Hansler and De Vries, 2019). Despite the US's threat, these countries continue to block domestic access to ICTs (King, 2019; Freedom House, 2023). A standard explanation for this blocking uses the domestic story of denying technologies that could increase internal unrest (Acemoglu and Robinson, 2006). But my account proposes that in settings like this, where the interests of potential interveners are sufficiently large, a plausible alternate explanation exists. Specifically, the Targets fear that cutting off access to covert operations may entice powerful interveners into overt actions, so they underinvest.

Implications

Proposition 3.1 and Figure 3 illustrate that blocking ICTs is most attractive for T when the intervener, A, is very powerful (i.e. p_O is high). Facing a smaller intervener (lower p_O), T would be less concerned about overt intervention. Additionally, a smaller intervener would be more likely to prefer no intervention, rather than overt, when T invests. If this were the case, the threat that causes T to block ICTs would no longer be credible.

Also, the mechanism of the underinvestment equilibrium implies that T is most likely to block when ICTs are very powerful for the types of monitoring that would expose covert operations. Otherwise, investing would not push A away from covert intervention.

However, the overall benefit of new ICTs (α) must be low relative to the danger of overt intervention (p_O). Otherwise, T would not be willing to sacrifice α by blocking. So, the absolute benefit of ICTs that T forgoes may vary, depending on the magnitude of the threat of losing power in an overt intervention.

These characteristics fit some of the relevant potential cases of underinvestment today. For example, the United States has a large military, making the chance of overt success substantial. However, it faces significant costs to overt military actions, and this has historically made covert operations a preferred policy (Carson, 2018). For targets of US intervention, ICTs that make covert intervention less feasible could encourage the US to instead use overt force against them.

3.2.1 Robustness

In this model, I assume that whether or not to invest in ICTs is a strict decision–T can either block ($z = 0$) or facilitate ($z = 1$). However, as I mentioned in Concepts, governments may overall take a middle approach, investing in ICT access and innovation but not fully. To portray this, we can also use a version of the model where ICT investment is a continuous variable; now, T can set z to any value from 0 to 1. In the appendix, I verify that this version produces similar predictions for blocking ICTs. The blocking conditions we saw in the baseline model now produce equilibria where T invests only partially in ICTs.

4 Extended Model: The Effects of ICTs on Covert Influence

In other literature, scholars have determined that domestic pressures can also cause technological underinvestment–economic backwardness–by encouraging governments to block developments that could endanger their hold on power. Perhaps the most prominent of this work is Acemoglu and Robinson, 2006. However, this has not been studied thoroughly in conjunction with international threats.[6] Is my logic of externally induced underinvestment different from domestically induced backwardness, in the context of ICTs? In this section, I integrate the domestic literature with my international threat model to answer this question.

First, I find that these mechanisms are distinct. The domestic blocking mechanism can emerge without any foreign threats (as Acemoglu and Robinson predicted), while the international mechanism for underinvestment requires a covert, foreign threat that can become overt. In the former, a state underinvests in, or blocks, technology that could help a dissatisfied public revolt and replace the regime. In the latter, a state underinvests in technology that could help expose covert operations; in doing so, it tolerates foreign covert operations to avoid overt intervention.

However, the mechanisms can also complement each other, because in the context of modern ICT investments and foreign intervention, foreign threats often operate *through* domestic politics. Specifically, a feature of ICTs is that they can assist covert operations by amplifying domestic unrest.

As I described in Concepts, interveners often use covert operations to influence domestic populations against their government, to help the intervener achieve its political goals within the target state. Even non-covert sources of international influence, like online news and social media, can support these goals. Covert influence also contributes to the appeal of covert operations as an indirect, limited, alternative to overt intervention.

So, while ICTs still make covert intervention vulnerable to detection, they have an additional effect on covert political influence operations, because interveners may use ICTs to better control information and exert influence. In these cases, ICTs could improve the efficacy of covert intervention, while still increasing its risk of being exposed. So, investing in ICTs may sometimes make covert action more, rather than less, preferable for interveners.

[6] Acemoglu and Robinson, 2006 do argue that external threats only discourage economic backwardness. However, they do not distinguish different types of foreign threats (like overt and covert).

4.1 Setup

I extend the model to introduce the public (M), which is similar to the "citizens" player in Acemoglu and Robinson's model. Unless stated otherwise, T and the intervener (A) have the same preferences as the initial model. Figure 4 represents the revised sequence of moves, with the payoffs listed in the table below. This is also a complete-information model, and my analysis uses sub-game perfect equilbria in pure strategies.

In the extended model, T first decides whether to invest in ICTs (*block* or *facilitate*), and then A decides whether and how to intervene (Overt, Covert, or No Action). If A chooses Overt (which succeeds with probability p_O), the game ends. If A chooses Covert, Nature (N) decides with probability $p_U(z)$ whether A remains undetected. If A is detected, intervention fails and the game ends.[7]

If A chooses No Action, M decides whether to replace T. Replacement is a costly lottery that determines whether M succeeds with probability p_R.[8] I also refer to attempted replacement as "domestic unrest" or "revolt." M's decision of whether to revolt depends on:

- Public support for T ($b \in [0, 1]$) and support for the government that would replace T ($1-b$)[9]
- The benefit of ICTs (α), which it would obtain after successful replacement, if T did not already facilitate ICTs[10]
- The probability of success (p_R)
- The cost of replacement ($w_z \geq 0$)

If A chooses Covert and remains undetected, M also decides whether to replace T. This time, however, covert influence has decreased M's support for T (now $b(1 - p_E(z))$), making M more likely to revolt.

[7] When covert intervention is detected, I assume that a rally-around-the-flag effect occurs which increases public support for T, negating the need for a replacement decision subgame for M.

[8] Choosing to replace could mean organizing a revolt, voting against T in an upcoming election, or using another domestic mechanism to remove T from power and replace them with a challenger. For now, I assume that replacing T involves some action that is not certain to succeed ($p_R < 1$). However, if T can be replaced through a free election, p_R would be 1 (and $w_0 = w_1 = 0$), and I discuss this special case later.

[9] b can be thought of as the portion of M that prefer T to a challenger who would come into power if T is overthrown. So 1-b is the remaining portion that supports the challenger.

[10] When T loses power, I assume that a Challenger comes to power. This happens after successful revolt or overt intervention. The Challenger has no moves and is not a player. However, in Acemoglu and Robinson, 2006's model, there is a "new ruler" player that fulfills the same function. As Acemoglu and Robinson theoretically prove, innovating (i.e. investing in ICTs) is a dominant strategy for any new ruler that replaces an incumbent (121). This is the basis for my model's assumption that when T is replaced, M always gets the benefit of ICTs (α).

I distinguish two effects that ICT investment has on covert intervention. $p_U(z) \in (0,1)$, the likelihood that covert intervention remains undetected, decreases when T facilitates ICTs. (So $p_U(z)$ is similar to the baseline model's $p_C(z)$). $p_E(z) \in (0,1)$, the extent to which covert intervention changes public opinion (i.e. the efficacy of covert foreign influence), increases when T facilitates ICTs. Therefore, unlike the baseline model, investing in ICTs does not necessarily discourage A from conducting covert intervention.

Thus, there are now multiple thresholds that covert intervention must meet to be "successful" (unlike the single lottery $p_C(z)$ in the baseline model). Covert intervention must first remain undetected, and then it must influence the public enough for them to change their replacement decision. If it does these two things, the public's replacement effort (revolt) must then succeed for covert intervention to have fully worked.[11]

As an example, suppose T blocks ICTs and A conducts covert action undetected (i.e. Nature chose $p_U(0)$). M's payoff to not revolting is $b(1 - p_E(0))$ and its payoff to revolting is:

$$[1 - b(1 - p_E(0)) + \alpha]p_R + b(1 - p_E(0))(1 - p_R) - w_0$$

Simplifying, revolt is a best response if: $b(1 - p_E(0)) \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$

For the analysis in Section 4.2, I now isolate the conditions under which revolting is a best response for M at each of its decision nodes.

When: (subgame)	M revolts if...	
T blocks ICTs and A plays No Action	$b \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$	(C1)
T blocks ICTs and A plays Covert and is undetected	$b(1 - p_E(0)) \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$	(C2)
T facilitates ICTs and A plays No Action	$b \leq \frac{1}{2}(1 - \frac{w_1}{p_R})$	(C3)
T facilitates ICTs and A plays Covert and is undetected	$b(1 - p_E(1)) \leq \frac{1}{2}(1 - \frac{w_1}{p_R})$	(C4)

Note: If C1 is true, C2 is also true. If C3 is true, C4 is also true.

The formal strategy profiles for T and A are the same as in the baseline model. The strategy profile for M is $s^M(r \in \{No\ Revolt, Revolt\}|z, a)$, and Nature's strategy profile is $s^N(n \in \{1 -$

[11] Since the probability that covert intervention succeeds now depends on the likelihood that the public successfully replaces T, I no longer assume that overt intervention is always more likely to succeed than covert intervention. This is because covert influence may only need to have a small effect to encourage the public to replace their government, especially if replacement is not costly. For example, if replacing the government means electing a new one, covert influence could succeed by encouraging a small number of voters to change their votes. Or, covert influence may help an already-strong rebel group organize protests and revolts.

$p_U(1), p_U(1)|z, a\}$, where $p_U(1)$ means covert intervention is undetected.

It is important to add that the subsequent examples and equilibrium plots will assume that $w_0, w_z > 0$ (and $p_R < 1$). This allows me to focus on situations where replacement is costly for M and is not a fully democratic process (where we often observe economic backwardness). However, the model would still work if $w_0 = w_1 = 0$ and $p_R = 1$, which would illustrate a state where replacing T is costless and based entirely on the public's choice–such as a democratic election. I will briefly discuss this special case and its implications for ICT underinvestment later.

4.1.1 Substantive Interpretation of Covert Intervention

There are two substantive points that I use to justify the model's assumptions. First, what distinguishes ICTs from other militarily salient technologies is their relationship with the public, which is often exploited by covert meddling. Many covert operations are conducted through this mechanism, making it salient to model. Thus, the model represents ICT investment, not technological investment overall.

To make "investment" specifically about ICT investment, the design of the extended model allows us to think of covert intervention as an operation in which a foreign government uses ICTs to manipulate public sentiment and encourage M to replace T. So, I assume that facilitating ICTs increases the efficacy of covert influence. However, I still assume that ICTs make covert operations more detectable (as in the baseline model). Finally, consistent with the domestic effects of ICTs highlighted in Concepts, I assume that facilitating ICTs lowers the cost of revolt for M.

For a substantive example of covert influence and ICTs, consider Russian election influence against the US. During the 2016 and 2020 presidential elections, Russia mounted campaigns to manipulate electoral outcomes by spreading misinformation online, often posing as political officials, discouraging voting, and targeting ideological divisions within both major political parties (Young, 2020). Russia was only able to do this because the United States has largely facilitated Internet access and social media (i.e. $z = 1$ for many of its investment decisions). As a result, the US became more vulnerable to covert influence.

Second, I make informational assumptions about the public. If Nature detects covert operations, I assume that there is enough direct evidence for T to prevent the effects of covert influence. At the same time, M responds to this evidence with a rally-around-the-flag effect in support of T

(Mueller, 1970; Baum, 2002).

However, this public reaction is based on elite cues, which often require direct evidence to generate. When no direct evidence of covert influence is observed, M's preferences may change, but M does not know whether it is in a world where successful covert action took place. In other words, after successful covert intervention, M has a different information set than it would if A chose No Action, yet it doesn't completely "know" that covert intervention happened.

This constraint is motivated by several factors. First, the public is not a party to the complex strategic process between states; rather, they react to external threats based on how these threats are presented (Myrick, 2021). If elite informational cues (such as national media reports highlighting covert operations) do not accompany covert exposure, the public may still know that their preferences have changed as a result of covert influence, but will not respond in a way that prevents covert influence from succeeding. Furthermore, without national elite cues, some individuals within M may recognize that influence occurs, while others may not (and ICTs can prevent this fragmentation from happening, increasing the risk of widespread exposure).

For example, the American public may have received such elite cues as more direct evidence of Russian interference amassed. However, while it was taking effect, they were less acutely aware of it.

Additionally, covert foreign influence is often supported by overt sources of information, like foreign news media and overt political messaging from foreign pundits, which can also influence domestic politics in favor of covert interveners. So, individuals in M may recognize the impact of foreign sources on their political positions, but not realize that these sources are playing a role in a foreign, covert influence operation. Underinvesting in ICTs can limit access to these sources, too.

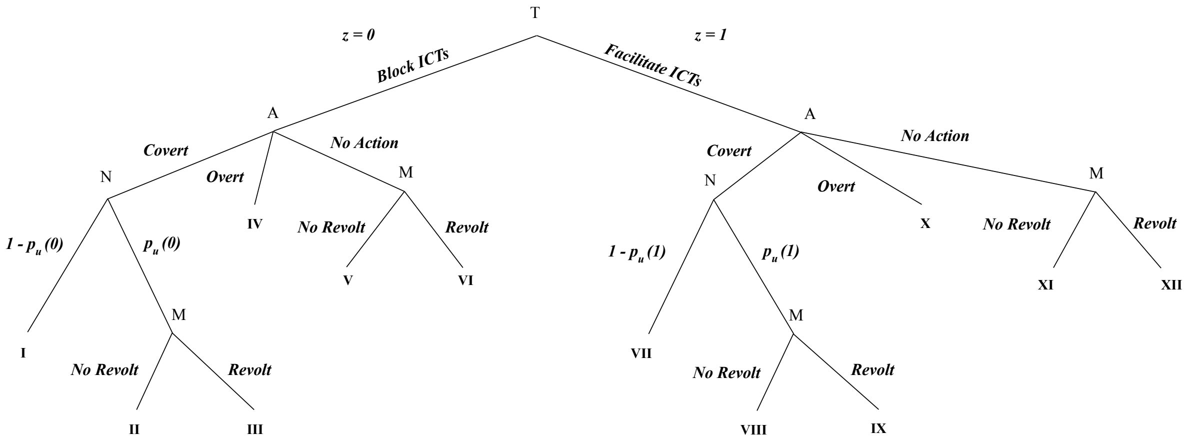


Figure 4: Extended Model Game Tree

Label	T's payoff	A's payoff	M's payoff
I	1	$-k_C$	b
II	1	$-k_C$	$b(1-p_E(0))$
III	$1-p_R$	p_R-k_C	$[1-b(1-p_E(0))+\alpha]p_R+b(1-p_E(0))(1-p_R)-w_0$
IV	$1-p_O$	p_O-k_O	$(1-b+\alpha)p_O+b(1-p_O)$
V	1	0	b
VI	$1-p_R$	p_R	$(1-b+\alpha)p_R+b(1-p_R)-w_0$
VII	$1+\alpha$	$-k_C$	$b+\alpha$
VIII	$1+\alpha$	$-k_C$	$b(1-p_E(1))+\alpha$
IX	$(1+\alpha)(1-p_R)$	p_R-k_C	$[1-b(1-p_E(1))]p_R+b(1-p_E(1))(1-p_R)+\alpha-w_1$
X	$(1+\alpha)(1-p_O)$	p_O-k_O	$(1-b)p_O+b(1-p_O)+\alpha$
XI	$1+\alpha$	0	$b+\alpha$
XII	$(1+\alpha)(1-p_R)$	p_R	$(1-b)p_R+b(1-p_R)+\alpha-w_1$

Parameter	**Interpretation**
$b \in [0,1]$	M's value of having T in government
$w_z \geq 0$	M's cost of replacing T (e.g. revolting)
$p_R \in (0,1]$	The probability that replacement succeeds
$p_U(z) \in (0,1)$	The probability that covert action remains unexposed
$p_E(z) \in (0,1)$	The amount that covert influence reduces M's support for T

Assumption	**Interpretation**
$w_1 \leq w_0$	It is easier to replace T if ICT investment has occurred
$p_U(0) > p_U(1)$	Facilitating ICTs (investment) makes it harder to conduct covert action undetected
$p_E(0) < p_E(1)$	Covert influence is more effective with better (facilitated) ICTs
$k_O > k_C$	Overt action is more costly than covert action

Note: Parameters not listed here are also in the baseline model and have the same characteristics here.

4.2 Results

Roadmap: The goal of this section is to illustrate three results of the extended model. First, I show that the model is consistent with existing predictions about domestically induced economic backwardness by producing similar results, under similar conditions, to Acemoglu and Robinson, 2006. As they also predict, I show that external threats generally encourage technological investment and discourage the blocking of ICTs (but not always).

I also demonstrate that the underinvestment prediction produced by my baseline model survives, under new conditions and through a mechanism different than in domestically induced underinvestment. Once again, this is important because it implies that underinvestment can occur under conditions that haven't yet been formalized. This result could guide empirical research, providing a possible explanation for observations of technological backwardness that cannot be explaiend by the existing domestic mechanism.

Finally, under yet another set of conditions, a new dynamic arises where the domestic and international threat mechanisms interact and encourage underinvestment in ICTs. While this dynamic appears similar to domestic economic backwardness, the "domestic" threat that causes the state to block ICTs here is actually caused by foreign influence. This prediction speaks to the importance of studying economic backwardness, especially in the context of ICTs, as a funciton of both domestic and international factors.

4.2.1 Robustness with Existing Theory and the Baseline Model

Consistent with the existing economic backwardness literature, the model supports several equilibria in which the fear of domestic unrest alone can cause the Target state to block ICTs.[12] This result is almost identical to Acemoglu and Robinson, 2006, and it occurs under similar conditions. Namely, T blocks ICTs when the probability of successful revolt (p_R) is high and the benefit of ICTs (α) is low. In these equilibria, T blocks ICT investments to avoid giving M technology that would make it easier for them replace T (i.e. w_1 is much smaller than w_0). Together, we can describe them as:

[12] My model supports five equilibria where T blocks ICTs to avoid domestic revolt. They mainly differ in the outcomes that T tolerates to avoid revolt (i.e. no foreign intervention or overt intervention). In Appendix A.1.5, I describe one of these equilibria.

Underinvestment (domestically induced): Any strategy profile in which:

- The target state blocks ICTs.
- Off the path (if the target had facilitated ICTs), domestic unrest occurs (i.e. M revolts).

I describe one such equilibrium in Appendix A.1.5.

Additionally, as the conventional wisdom assumes, the model predicts that external threats often encourage ICT investment. In the extended model (as in the baseline model), when facilitating ICTs has no effect on the on the type of foreign intervention A conducts, T can easily increase its payoff by investing in ICTs (adding α, conditional on staying in power). When the unchanging foreign threat that T faces is covert, facilitating ICTs is even better, because it also increases the chance that covert operations are detected.

The underinvestment mechanism highlighted by the baseline model also emerges in the extended model. In fact, the model supports four equilibria in which T blocks ICTs to avoid an overt intervention by A.[13] However, covert intervention now refers only to covert operations that manipulate public sentiment, a narrower set of operations than implied by the baseline model. Thus, when T tolerates covert intervention in these equilibria, it is specifically tolerating this type of operation. We can describe these equilibria together as:

Underinvestment (externally induced): Any strategy profile in which:

- The target state blocks ICTs.
- Off the path, the intervener intervenes overtly.

I describe these equilibria in Appendix A.1.6. Two of these equilibria closely resemble the baseline model's externally-induced underinvestment mechanism. In both, facilitating ICTs has the primary effect of making covert intervention more vulnerable to exposure, while having a smaller positive effect on the efficacy of covert influence. This makes covert intervention advantageous for A when T blocks ICTs, but not when T invests in them. If T invested, A would instead conduct overt intervention. As a result, T blocks ICTs, allowing it to avoid overt intervention but forcing it to face covert intervention, which, if undetected, may cause domestic unrest.

The other two external underinvestment equilibrium also involve T blocking ICTs to avoid overt intervention. However, in these cases, T tolerates domestic unrest when it blocks ICTs, not covert

[13] These equilibria, E1-4, are described in Appendix A.1.6. E1 and E2 are formally defined, and I briefly describe E3 and E4.

intervention (which does cause domestic unrest, but only if undetected). How can this occur? In these two equilibria, M is sufficiently dissatisfied with T, and the benefit of ICTs is sufficiently high, that M will revolt when T blocks ICTs–even if it has not been covertly influenced to do so. So, when T blocks, A does not need to conduct covert intervention to convince M to revolt.

However, when T facilitates ICTs, M has fewer incentives to revolt. With M no longer revolting on its own, A must intervene overtly or covertly (if C4 is true) if it wants to overthrow T. In these two equilibria, A prefers overt intervention, and to avoid this, T blocks ICTs and faces domestic unrest.

Implications

As was the case in the baseline model, the main mechanism for externally-induced underinvestment in ICTs is the promise of overt intervention should T facilitate ICTs. This promise is genuine when A is powerful (p_O is high), because once ICTs are improved, it is harder for A to effectively intervene covertly, which it previously preferred, and overt intervention is its next best option. This mechanism exists in both types of external blocking described above.

Also, the conditions for external underinvestment are clearly distinct from those of domestic backwardness. In the domestic mechanism, T is threatened by the fact that facilitating ICTs would help M revolt. This implies that ICTs significantly reduce the cost of revolt (w_z) for an already dissatisfied M. If T blocks, M may want the benefit of ICTs, but is deterred by the high cost of revolting (w_0), which it must incur to get ICTs.

In the external mechanism, T is instead threatened by overt intervention. Also, the cost of revolting without ICTs (w_0) must be low enough that M would revolt when T blocks, or could be covertly convinced to revolt by A. And, for external blocking to occur, the benefit of ICTs (α) must be high enough that once T facilitates them, M no longer finds it beneficial to revolt.

4.2.2 Underinvestment in ICTs as a Result of Both Foreign and Domestic Threats

The model also illustrates a new dynamic in which the threat of foreign covert intervention complements the threat of domestic unrest, causing underinvestment in ICTs. These cases look like examples of traditional domestic economic backwardness. However, they occur under different conditions than either the domestic or external mechanisms, and are only reachable when both domestic and foreign threats exist. The model supports two such equilibria, which I define together as:

Underinvestment (hybrid): Any strategy profile in which:

- The target state blocks ICTs.
- Off the path, the intervener conducts covert intervention, which could lead to domestic revolt.

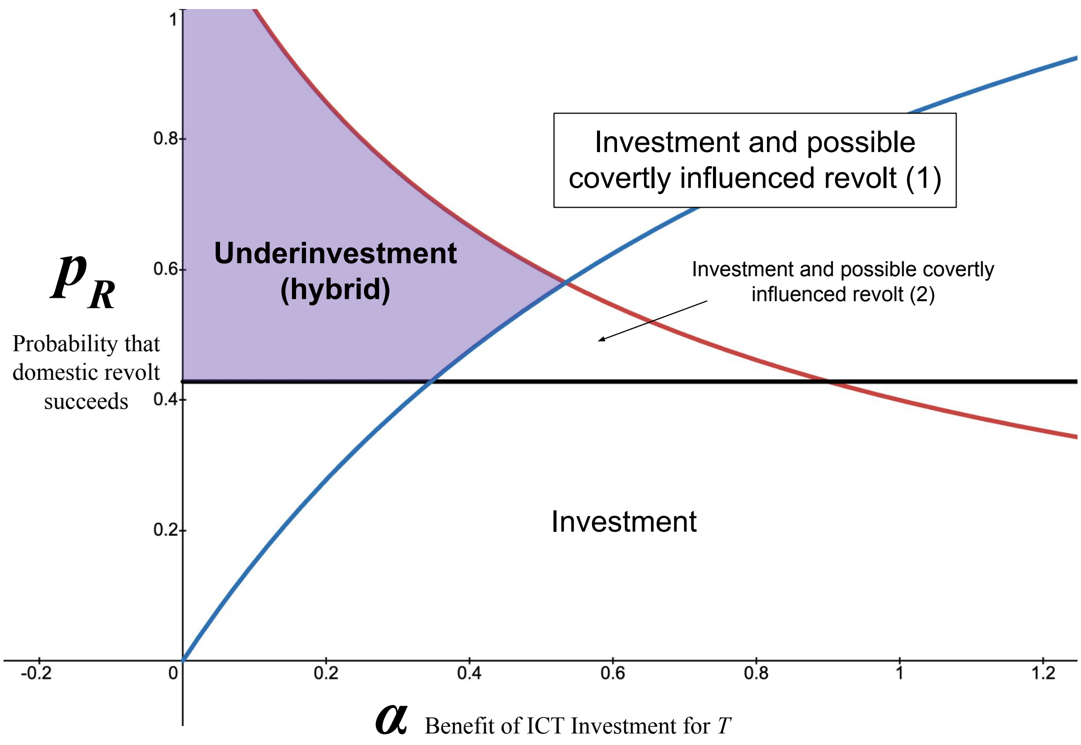


Figure 5: Equilibria as a function of p_R and α

Notes: Assumes $b = 0.5, p_O = 0.4, k_O = 0.6, w_O = 0.6, w_1 = 0.3, p_E(0) = 0.5, p_E(1) = 0.7, p_U(0) = 0.8, p_U(1) = 0.6, k_C = 0.1$.

Equilibrium	On-Path Actions	Off-Path Actions
Underinvestment (hybrid blocking)	T blocks ICTs; A plays No Action; M does not revolt	If T facilitated ICTs, A would play Covert and M would revolt if A is undetected
Investment and possible covertly influenced revolt (1)	T facilitates ICTs; A plays Covert; M revolts if A is undetected	If T blocked ICTs, A would play Covert and M would revolt if A is undetected.
Investment and possible covertly influenced revolt (2)	T facilitates ICTs; A plays Covert; M revolts if A is undetected	If T blocked ICTs, A would play No Action and M would not revolt
Investment	T facilitates ICTs; A plays No Action; M does not revolt	If T blocked ICTs, A would play No Action and M would not revolt

According to the existing understanding of domestic economic backwardness (including this model's domestic blocking equilibria), a government will block technological change if allowing it would give citizens the means to replace the regime. This requires that the public wants to replace their government in the first place, but are unwilling to do so until better technologies arrive that reduce the costs of revolting.

As I described in Concepts, ICTs represent a technology that can reduce the cost of revolting, by helping organize protests and recruit citizens against the government. But ICTs are also a tool foreign powers use to manipulate domestic citizens against their regime–thus influencing the domestic unrest that compels the government to block technology. In other words, because ICTs allow foreign threats to incite domestic unrest, foreign actors can contribute to the overall threat of domestic replacement that induces a target state to block ICTs.

The model illustrates this mechanism by allowing A to reduce M's support for T if it successfully conducts covert intervention. Under certain conditions, M's support for T is too high to incentivize revolt–unless A conducts covert intervention first, lowering support for T and making revolt look more appealing to M. This dynamic can compel T to block ICTs. In these cases, facilitating ICTs would improve A's ability to covertly influence M, and would reduce the cost of revolting enough that covert intervention could cause domestic unrest. T may block ICTs to avoid this potential unrest. I characterize one case below.

Proposition 4.1 *Suppose C4 holds. If $p_U(1)p_R - k_C \geq 0 \geq p_O - k_C$ and $1 \geq (1 - p_U(1)p_R)(1+\alpha)$, the following strategies are sub-game perfect. T blocks ICTs. A selects No Action if T blocked and Covert intervention if T facilitated. M revolts if T facilitated and A conducted Covert intervention undetected. Otherwise, M does not revolt.*

On the path, we observe ICT underinvestment, no foreign intervention, and no domestic unrest. Off the path ($z = 1$), we would observe investment, covert intervention, and possible revolt. [14]

Proposition 4.1 is proven in Appendix A.1.7, and the logic of the equilibrium is as follows.

Because only C4 is true, M only revolts if T facilitates ICTs (making it easier to revolt) and if A conducted covert intervention (lowering M's support for T). Overt intervention is never a good

[14] Proposition 4.1 and Figures 5 and 7 refer to the same hybrid underinvestment equilibrium, Hy1. Not pictured or described is equilibrium Hy2, which is similar to Hy1, except when T blocks ICTs, it faces Overt intervention, which it prefers to facilitating ICTs and facing possible covertly influenced revolt. This equilibrium requires that p_O be very low compared to $p_U(1)p_R$, and/or that α be very low. Hy2 is briefly distinguished in Appendix A.1.7.

option for A. When T facilitates ICTs, however, A can use covert intervention to influence M to replace T, and for A this is better than taking no action. Fearing covertly-influenced domestic unrest as a result of facilitating ICTs, T blocks ICTs to avoid this outcome.

As Figure 5 illustrates, some of the conditions for hybrid underinvestment resemble conditions for domestic underinvestment. The probability of successful revolt (p_R) must be high enough that covert intervention can convince M to revolt, but not so high that M would revolt without covert influence or facilitated ICTs.[15] And, as with all other underinvestment equilibria, as the benefit of ICTs increases, T becomes less willing to block them. However, unlike the domestic result, covert intervention is preferable for A if T facilitates ICTs, because it can convince M to revolt.

To summarize, hybrid underinvestment occurs when facilitating ICTs would cause A to conduct covert intervention, which could lead to revolt. From the outside, this case might look like domestic backwardness, and its logic is similar, since T avoids giving M technology that would help with revolt. However, the ICTs that T blocks would allow foreign powers like A to covertly stir up public discontent, creating the unrest that threatens T. In practice, because successful covert influence happens secretly, the role of foreign powers in encouraging technological underinvestment may not be immediately visible. However, it is essential for this hybrid mechanism to occur.

By distinguishing between covert and overt intervention and the conditions in which an intervener uses each policy, we paint a nuanced picture of the effects that external threats have on economic backwardness in ICTs. In many cases, external threats encourage governments to invest more in ICTs, as the conventional wisdom suggests. However, external threats can disincentivize ICT investment in two ways. In externally induced underinvestment, a government blocks ICTs to avoid facing overt intervention, and instead tolerates foreign covert intervention. In hybrid underinvestment, a government blocks ICTs that would allow foreign powers to covertly influence the public and produce domestic unrest.

[15] When p_R increases, T's post-innovation payoff falls, further encouraging T to block ICTs. However, also as p_R increases, M is more likely to revolt when T blocks ICTs, too. If this becomes the case, T would prefer to facilitate ICTs. These competing effects explain why increasing p_R sometimes makes hybrid underinvestment more likely, and at other times makes it less likely, in Figure 5.

4.2.3 The Competing Effects of Covert Exposure and Efficacy on ICT Underinvestment

In the extended model, facilitating ICTs has two effects on covert operations: it makes them easier to detect (by decreasing $p_U(z)$) and it makes them more effective at influencing domestic politics (increasing $p_E(z)$). So, unlike the baseline model, facilitating ICTs doesn't necessarily make covert intervention less attractive for A. That depends on which of the two effects is stronger. As I explain below, these two effects each impact external and hybrid underinvestment differently.

Effect of ICTs	Makes Underinvestment (External)...	Makes Underinvestment (Hybrid)...
Improve detection	More likely	Less likely
Improve ability to influence domestic public	Less likely	More likely

If facilitating ICTs mainly makes covert influence more susceptible to exposure (i.e. the decrease from $p_U(0)$ to $p_U(1)$ is more influential than the increase from $p_E(0)$ to $p_E(1)$), then we should expect to see external underinvestment under similar conditions as the basline model, since $p_U(z)$ affects covert intervention in the same way $p_C(z)$ did there. On the other hand, if facilitating ICTs primarily allows A to better influence M (i.e. the increase from $p_E(0)$ to $p_E(1)$ is stronger), A would be more likely to prefer covert intervention when T innovates. If this is the case, T would not be threatened by overt intervention anymore, allowing it to facilitate ICTs.

Figure 6 illustrates these effects, plotting equilibria as a function of $p_U(1)$, $p_E(1)$, and p_O.[16] As the right plot shows, as $p_U(1)$ increases (i.e. covert intervention remains sufficiently undetectable when T facilitates ICTs), covert intervention is more likely to continue after T facilitates, so T is less likely to block ICTs. However, if $p_E(1)$ is not high enough (left plot), A cannot covertly influence M to revolt when T invests, so blocking can occur regardless of $p_U(1)$.

While the conditions for external underinvestment may now be narrower than in the baseline model, the extended model also yields hybrid underinvestment. In this result, covert intervention is part of the threat that compels T to block, instead of the "lesser evil" that T tolerates while blocking ICTs (which was the case in external underinvestment). So, any effects that ICTs had on

[16] Equilibria E2 is plotted in the left plot of Figure 6 and E3 on the right plot. They have the same on-path results, and both contain overt intervention off-path (i.e. when T facilitates ICTs).

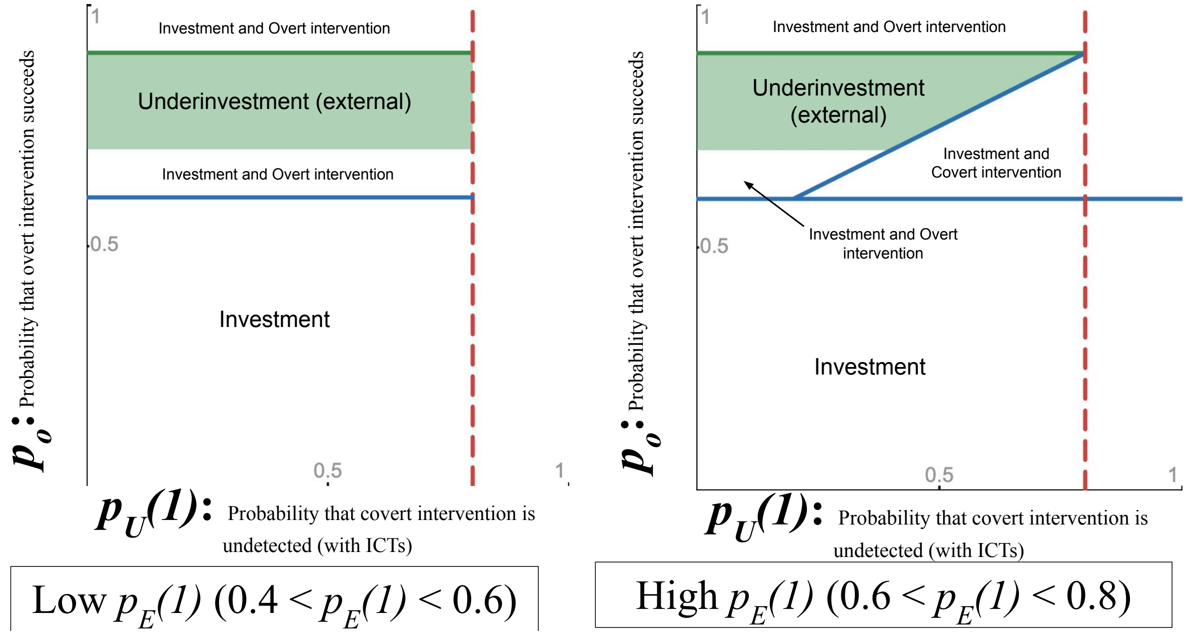


Figure 6: Equilibria as a function of $p_U(1)$ and p_O

Notes: Assumes $b = 0.5, k_O = 0.6, p_R = 0.5, w_O = 0.6, w_1 = 0.3, p_E(0) = 0.4, p_U(0) = 0.8, \alpha = 1, k_C = 0.1$.

external underinvestment will impact hybrid underinvestment in the opposite direction.

Thus, when the other conditions for hybrid underinvestment are in place, an ICT with the primary effect of increasing detection of covert operations will make covert intervention less appealing to A once T facilitates. If this means that A no longer conducts covert intervention, M could not be influenced to revolt, encouraging T to facilitate ICTs. Conversely, an ICT that primarily improves A's ability to manipulate M with covert operations will make such operations more appealing to A after T facilitates–encouraging T to block it.

Figure 7 illustrates equilibria as a function of $p_U(1)$, $p_E(1)$, and p_R. As $p_U(1)$ increases, so does the likelihood of hybrid underinvestment. This is because, when $p_U(1)$ increases, detection is less likely; so A is more likely to conduct covert intervention when T facilitates, and less likely to conduct no action.

When $p_E(1)$ is high, A can more effectively use covert intervention to influence M (after T facilitates ICTs), so hybrid underinvestment becomes more likely. When $p_E(1)$ is low, A may not be able to effectively influence M with ICTs. If this is the case, M would never revolt, so blocking cannot occur.

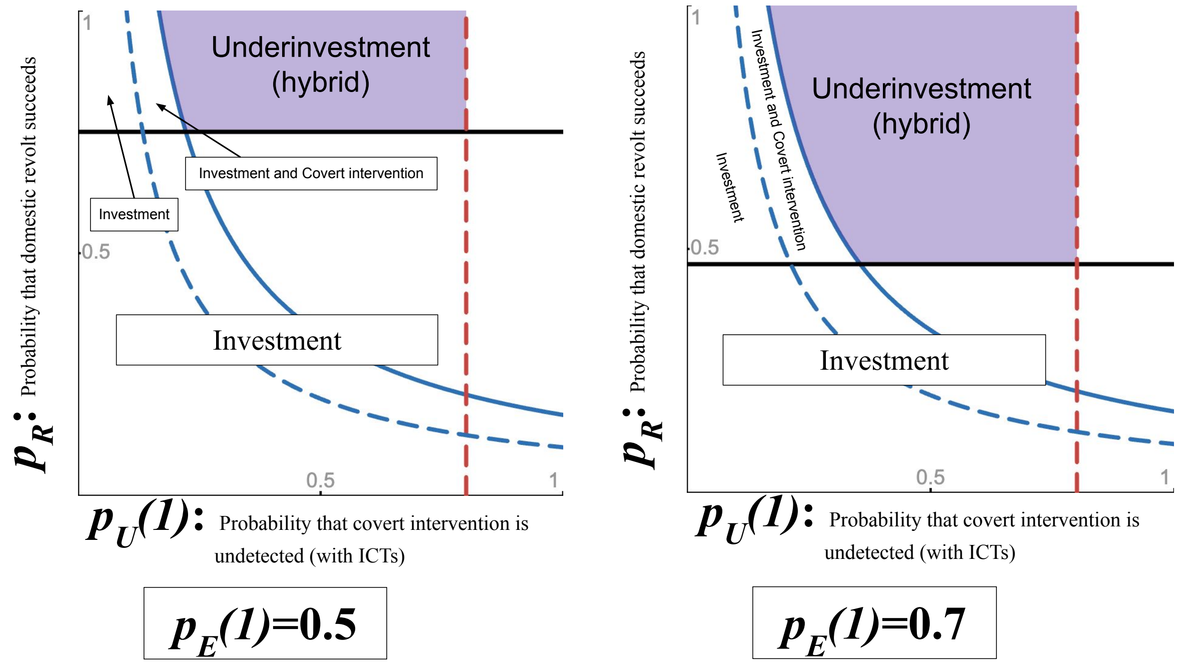


Figure 7: Equilibria as a function of $p_U(1)$ and $p\alpha$

Notes: Assumes $b = 0.6, p_O = 0.4, k_O = 0.6, w_O = 0.6, w_1 = 0.3, p_E(0) = 0.4, p_U(0) = 0.8, \alpha = 1, k_C = 0.1$.

4.3 A Note about the Model and Democracies

So far, I have focused on parameter ranges that best reflect the Target states as autocratic regimes. Specifically, when the public decides to replace their government, it is costly ($w_0, w_1 > 0$) and is not certain to succeed ($p_R < 1$); I have thus called this the decision to revolt. Ordinarily, we might think of autocracies as especially vulnerable to economic backwardness, as leaders can evade some accountability for unpopular policies that deny citizens access to technology. This characterisation also resembles the most typically referenced cases of backwardness, including the historical regimes Acemoglu and Robinson profiled.

However, we can also use the model to illustrate a democratic state, where the public's replacement decision is an election. The public (M) now represents a normalization of all voters, who jointly decide whether to reelect or replace T. We can set $p_R = 1$, so if M chooses to replace T, they automatically do so successfully. And $w_0 = w_1 = 0$, since all M must do to replace T is vote against them. As before, I assume that any challenger would invest in ICTs once elected, if T did not already do so.

M no longer must consider the costs and likelihood of success when deciding whether to replace

T. These constraints allow us to update the conditions under which M replaces T:

- When T facilitates ICTs and no foreign intervention occurs, M replaces T if $b \leq 0.5$ – in other words, if a majority of M opposes T.
- When T blocks ICTs and no foreign intervention occurs, M replaces T if $b \leq 0.5(1 + \alpha)$. In other words, when replacing T means getting better ICTs (α), some voters in M who slightly preferred T would instead vote for the challenger because of the preferable policy (ICT investment) they would implement.
- In either of the above cases, foreign covert intervention would reduce the subset of M that supports T, from b to $b(1 - p_E(z))$. This can be interpreted as: covert influence convinces some former T supporters to instead vote for challenger, and/or encourages nonvoters to become voters for the challenger.

Applying these parameters overall narrows down the number of reachable equilibria where T underinvests, with interesting results:

Result 1: When the public's replacement decision represents an election, there are no equilibria where domestic threats alone cause the government to deny ICT access.

In other words, democratic governments who face no external threats of covert operations or influence, should always facilitate ICTs. This is consistent with Acemoglu and Robinson's logic, which showed that elites blocked innovation when doing so would cause institutional instability that decreased the public's cost of replacing them. Under democratic parameter ranges in this model, replacing the elites just entails voting them out of office, which has no cost regardless of whether the elites have blocked or innovated. Thus, innovating does not erode elites' authority or incumbency advantages.

However, in the real world we still see examples of technological underinvestment in democracies (Freedom House, 2023). A second result of the model suggests one reason for this observation:

Result 2: International threats can induce underinvestment in democracies, through both the externally-induced mechanism and the hybrid mechanism in which T blocks ICTs to avoid foreign-influenced domestic unrest.

Even though ICTs no longer affect M's cost of replacing T, they can still impact foreign covert intervention. Facilitating ICTs can increase detection capabilities, rendering covert intervention unfeasible and driving interveners into overt actions–so the possibility for external underinvestment remains. Or, facilitating ICTs may have the primary effect of improving covert influence, making it possible for interveners to "convince" M to elect a challenger–so the conditions for hybrid underinvestment also remain.

Hybrid underinvestment in democracies is especially interesting, as the Internet has allowed interveners to covertly meddle in democratic elections. Further theoretical and empirical research could generate more detailed conditions under which democratic governments block ICTs to prevent covert election meddling.

5 Empirical Implications

5.1 Implications for Cross-national Studies

A number of general implications follow from the model that will be useful to empirical scholars, and they add interesting predictions to existing theory. According to Acemoglu and Robinson, 2006, in a world where leaders face no domestic threats, states will never block access to technology. My model, however, implies that even when the public is supportive of the government, there may still be technological underinvestment, specifically, in the ICT sector.

This underinvestment occurs because of foreign threats. Acemoglu and Robinson's theoretical argument suggested that external threats always encourage investment in ICTs. My models show that this is usually the case, but there are scenarios where this common prediction is insufficient.

First, I create a prediction consistent with my model and robust to previous backwardness theory:

Implication 1:

A *When a target state is unlikely to receive covert intervention from its adversaries, and there are minimal domestic threats, it will invest in ICTs. As the size of overt external threats increase, ICT investment is even more likely.*

B *However, if improved ICTs could fuel domestic revolt, the state may block ICTs.*

Based on my analysis of underinvestment as a result of the threat of overt intervention, I generate the following new prediction:

Implication 2:

A *If a state faces a very powerful foreign adversary that prefers to intervene covertly against them, the state may block ICTs. As the adversary's relative power increases, blocking becomes more likely.*

B *The state may specifically block ICTs that help monitor and detect covert operations.*

Blocking ICTs seems counterintuitive, since ICTs help against covert attacks. However, target states block them to avoid inducing overt intervention against them, and to keep their international threats within the less costly covert theater.

Specifically, when an intervener is powerful, overt intervention against a target state will be very likely to succeed, so they would probably prefer to attack targets overtly (rather than not at all) if improved ICTs push covert operations off the table. If a target state has a lower base level of ICTs and a powerful intervener prefers covert intervention, the target may be able to avoid overt intervention, by blocking ICTs and allowing covert intervention to occur undetected. The more dangerous overt intervention becomes (i.e. the intervener's power advantage increases), the more likely it is that the target will block.

This implication is especially important because it modifies Acemoglu and Robinson's prediction about economic backwardness. It suggests that states may underinvest in ICTs even in the absence of the threat of domestic rebellion. This emphasizes the need for empirical research into the international determinants of technological underinvestment.

Based on my analysis of underinvestment as a result of complementary domestic and foreign threats (hybrid blocking), I generate the following prediction:

Implication 3:

A *If a state faces considerable domestic unrest and a foreign intervener capable of covert influence, the state may block ICTs.*

B *The state may specifically block ICTs that improve international communication and foreign covert influence.*

Some ICTs, particularly those related to the Internet, can make foreign covert influence campaigns more effective at reaching domestic citizens. When there exists political opposition that could be exacerbated by foreign influence, limiting these ICTs may prevent the opposition from growing and endangering the regime. This prediction also provides nuance to Acemoglu and Robinson's backwardness prediction; specifically, it suggests that the threat of domestic revolt can be complemented by foreign powers. Under this mechanism, foreign threats can actually lead to underinvestment.

This implication once again emphasizes the importance of studying modern ICT investments in the context of foreign, in addition to domestic, threats. It suggests that empirical scholars should consider the impact of foreign threats on underinvestment, even when domestic pressure exists that could explain a state's blocking of ICTs. In particular, we should consider the complementary effect of foreign threats on domestic pressure through ICTs.

Cross national studies testing these predictions are beyond the scope of this paper, but further research could use these implications to determine in detail the prevalence of foreign-induced economic backwardness in the context of ICTs.

5.2 Implications for Causal Mechanism Investigation

To test the models' causal mechanisms within case studies, we must first define the makeup of a case. The model suggests that a potential case of ICT underinvestment would not be a country overall, but rather a scenario where a country is faced with the policy decision of investment in ICTs or not. For example, this scenario could span the period after which a new technology is invented, during which a country decides how to make policies regarding the technology. Often, governments have multiple opportunities over long time periods to choose and implement these policies. The model encourages me to identify these key decision points, and to determine whether, and why, the state chose to restrict or expand ICT access at each point.

Overall, my model illuminates a number of causal mechanisms for ICT underinvestment at these decision points, based on the fear of internal, external, or combined threats. These equilibria arise under different parameter ranges and each has a subtly different mechanism. Here I am going to identify the mechanistic predictions about a particular underinvestment prediction–the hybrid equilibrium.[17]

I chose to investigate the hybrid prediction further for several reasons. First, Acemoglu and Robinson's theory of backwardness can already be applied to my model's predictions about ICT blocking induced purely by domestic pressure. Second, out of my two novel predictions–blocking due to external threats and blocking due to the threat of foreign-influenced unrest (hybrid)–the latter

[17] Specifically, I describe equilibrium Hy1.

seems more empirically plausible. Third, the mechanism that leads to this result is substantively interesting and highlights the importance of studying economic backwardness as a function of both domestic and international events.

The conditions under which this equilibrium occurs are the following:

- Among a state's domestic public, there is dissatisfaction with the regime, and a potential for unrest.
- A foreign power, an adversary, opposes the state's regime but has not yet intervened in a way that severely threatens the regime.

Given that these conditions are met, my theory makes mechanistic predictions at two key points:

- When given the opportunity to invest in ICTs, the government makes a choice that underinvests in ICTs, to the detriment of the economy and public welfare. Both international and domestic concerns motivate their decision.
- If underinvestment did not occur, ICTs would threaten the government by facilitating domestic unrest and enabling foreign covert influence, which could increase that unrest.

My mechanistic predictions would be violated if the government in question primarily took actions to facilitate and expand ICTs across each of its decision opportunities. Further, even if the government did make policies that substantially blocked ICTs, my theory of hybrid blocking gives a very specific reason for why they deny them: to avoid foreign influence that could amplify existing domestic opposition and endanger the regime. If a government blocked ICTs but cited exclusively domestic or international concerns as their motivation, my theory would also be proven wrong. Finally, if the government only blocked ICT technologies that would not have clearly improved domestic unrest and foreign influence, the mechanism would also be invalidated.

6 ICTs in Iran

I now examine my qualitative predictions in the context of Iran's ICT investments, using the United States as its adversary. Following Bates, 1998, I pick a substantively interesting case where the initial conditions (listed in Section 5.2) match the underlying parameters where I expect the novel hybrid blocking equilibrium to occur. I validate those conditions in Section 6.1. Once validated, I select examples of ICT policies in Iran and code them as blocking or facilitating ICTs (6.2). Then in 6.3, following best practices in the evaluation of formal models (Goemans and Spaniel, 2016), I work through key decision nodes in the model and verify that the case's characteristics follow what I expect players to do in the model. In particular, the two questions I need to verify are:

- When the Iranian government has an investment opportunity relating to ICTs, do they forgo the opportunity (block)? Do they consider the threat of international covert influence when making their investment decision, or just domestic opportunities and pressures? (My theory would be invalidated if Iran always invested/facilitated ICTs, or if they underinvested but were motivated to do so by domestic or international conditions only.)
- Does the security threat to Iran posed by an adversary include the threat of covert influence, and could ICTs improve the efficacy of these operations at influencing the Iranian public?

6.1 Validating the Initial Parameters

To meet the initial criteria for hybrid underinvestment (5.2), Iran must be facing both internal and external threats. We can see that this is true for multiple reasons.

First, the hybrid equilibrium requires that there is existing public discontent with the target government, but not enough to easily overthrow the regime (i.e. b is not close to 1, and not close to 0 unless w_0 is very high). We see this in the Iran case, where public unrest over the last few decades suggests that Iranians are dissatisfied with their government. However, these movements did not severely endanger the Iranian regime.

The largest instance, the Green Movement of 2009-10, saw millions of protesters demonstrate in Tehran, disputing the government's swift announcement that the sitting president had won reelection (Milani, 2010). In 1999, a movement emerged among Iranian students, beginning as a protest for press freedom (Gorgin, 2008). Large protests also occurred in late 2017-18 and late 2019, drawing hundreds of thousands of demonstrators (Fathollah-Nejad, 2022). Most recently, the 2022-23 protest movement saw Iranians participate in thousands of anti-government demonstrations across the country (Dubowitz, 2023).

Additionally, polling suggests that many Iranians would prefer a secular regime to the current theocratic one (Aarabi et al., 2022). Similarly, decreasing turnout in recent elections signifies widespread "voter discontent" (Sharifi, 2024).

While these examples demonstrate significant opposition to the government, the scale of each movement has not nearly been sufficient to overthrow the regime, and they have not resulted in significant political reform. Instead, their outcomes largely illustrate the high costs of expressing dissent. In the 1999 student movement, more than a thousand were detained and dozens of students disappeared; although the movement did inspire later protests, no major political progress was made (Human Rights Watch, 1999; Maloney, 2013). During the 2009 protests, over one hundred protest leaders were arrested, thousands were detained, and dozens were killed; Iran's regime also responded with tighter restrictions on the press and Internet (BBC, 2009; Milani, 2010). During the 2019 protests, an estimated 1,500 were killed (Amnesty International, 2020). Tehran violently responded to the 2022-23 protests, as hundreds were killed and thousands arrested (Loft, 2023). The government also took measures to suppress the press and public figures and intensified restrictions on Internet access during parts of these protests–which ultimately have not eroded the regime's power (Castro, 2024; Hafezi, 2023).

The hybrid equilibrium also requires that the Target have a powerful foreign Intervener that prefers not to intervene unless the Target invests more in ICTs, at which point it could conduct successful covert influence (i.e. $0 \geq p_O - k_O$; $p_U(1)p_R - k_C \geq 0$; and only C4 holds). We see this in the case of Iran, which has powerful international adversaries. One source of these adversaries' threat, in the perception of Iranian leaders, is covert influence on Iranians, through ICTs. I focus on the United States as a powerful adversary and potential intervener against Iran. Currently, the US does not directly intervene against Iran's regime, but conflicts involving Iran suggest its potential willingness to do so. This matches the characterization of an adversary in the hybrid blocking equilibrium.

The US has covertly intervened against Iran in the past. In 1953, a coup covertly assisted by the US and UK overthrew Iran's then-prime minister (Byrne, 2013). During Operation Olympic Games, the US and Israel ran cyberattacks to disrupt the Iranian nuclear program. Olympic Games culminated in 2010, when the computer program Stuxnet disabled centrifuges used for uranium enrichment (Sanger, 2012). Additionally, reports suggest that the CIA had contacts with protesters during Iran's Green Movement (Lake, 2016). Although the US ultimately did not use these contacts to support the uprising, their presence suggests that the US could use covert support to influence politics in Iran.

Meanwhile, research suggests that foreign adversaries including the US are unlikely to overtly intervene against Iran. During the Iraq War, Iran covertly assisted Shiite insurgents in Iraq, and the US detected these activities early in the conflict. However, as Carson, 2018 demonstrates, American officials decided not to announce their awareness of Iranian intervention, and instead "colluded for several years to help control the scope of the war" (292). Carson uses statements from policymakers which suggest that Washington, concerned that "going public" (293) with its knowledge would force the US into a more direct, overt confrontation with Iran, preferred to continue fighting covertly (293).[18] Since then, it remains likely that the US wants to avoid a direct conflict with Iran, due to public disapproval of such a conflict and the difficulty of previous operations in the region (Kiley and Dougherty, 2023; Thrall, 2017; Kamarck and Muchnick, 2023; Shortridge, 2021; Smeltz et al., 2022).

At the same time, the US has been involved with overt conflicts against Iran and its proxies in the Middle East, and has conducted targeted attacks against Iranian military leaders. However, its aims in these conflicts are not to overthrow Iran's government altogether, and some of these attacks are in response to forceful overt actions by Iran (Harmeet et al., 2020; Pietsch, 2024; Global Conflict Tracker, 2024). Additionally, in recent covert operations (like Stuxnet), the US's activities did not directly attempt to overthrow Iran's regime. Therefore, current conflicts between the US and Iran do indicate the US's opposition to Tehran and willingness to intervene, but they would not likely meet the criteria for a direct overt or covert intervention as described in the models.[19]

6.2 Did Iran Block ICTs? Coding Selected Events

I list seven recent policies in which the Iranian government expanded or restricted ICTs. I code the policies as either blocking or facilitating of ICTs.

As Table 1 demonstrates, the Iranian government has both taken steps to expand and restrict particular aspects of ICTs. Ultimately, it provides several major examples of underinvestment that

[18] Carson demonstrates that Iran also wanted to avoid overt escalation with the US, and preferred to continue its covert support of Shiite militias in Iraq. However, if the US made it harder for Iran to continue its covert activities unexposed, would Iran have opted to take a more overt approach? If the US did not want this outcome, it could have taken steps (including ICT restrictions characteristic of this paper's external underinvestment prediction) to prevent Iranian intervention from being exposed to the public (although not necessarily undetected, since the US had already become aware of the covert action privately). Did policymakers in Iraq limit ICTs that could expose Iranian intervention to the broader public? Further research could examine governments in Iraq during this time to answer this question.

[19] More on this in Section 6.5.1.

Years	ICT Policy	Coding
Since 1990s	Iran allows Internet Service Providers (ISPs) to open when it first goes online, and now has over a thousand private-sector ISPs. The government regulates mobile service providers, but Iranians can broadly use mobile phones.	Facilitating
Since 2000s	Iran heavily imports computers and media technology, and encourages domestic technology production and development.	Facilitating
2001	Iran's Supreme Council of the Cultural Revolution (SCRC) requires ISPs to use "filtering" systems. Over the next few years, Iran's government concentrates its control of the Internet in Iran and conducts its own filtering.	Blocking
Since early 2000s	Iran has reduced Internet speeds or shut down Internet/mobile phone services during elections and protests, disrupting economic activity. The regime can control very specifically how well/quickly Iranians can use phones and the Internet. Major instances: 2006; Election/protests in 2009 and 2018-19 and protests in 2022-23	Blocking
Since mid 2000s	Iran filters or blocks access to social media sites, including X (formerly Twitter), Telegram, Facebook, Youtube, and Instagram. Prominent international media sites, like the New York Times and BBC, are also banned from the domestic Internet.	Blocking
Since 2005	Iran's Fourth Five-Year Development Plan aims to encourage technological innovation in the private sector. The Fifth Plan encourages science and technology innovation in Iranian universities. The Sixth plan aims to expand connection to the National Information Network.	Facilitating
Since 2005	Iran begins developing the National Information Network, a domestic version of the Internet managed by the state. The Network helps the government reduce Internet speeds, filter foreign websites, and monitor online activity.	Blocking

Table 1: Coding ICT Policies

These policies are described, with sources, in Appendix A.2.

could be represented as blocking in the model.

The ICT policies shown in the table can be considered backward because they forego social and economic benefits that alternative policies would generate, and have hampered technological innovation (Anderson, 2016). The government's ability to effectively turn off sections of the Internet, or at least restrict Internet use, risks interfering with banks and impeding "internet commerce," while local officials have admitted that slow Internet speeds disrupt everyday online business (Tajdin, 2013; Rezaian, 2023). Additionally, Iran's National Information Network risked interfering with foreign investment in Iran, and by creating a network detached from the global Internet, Iranian officials sacrificed access to the "expertise and resources" of existing technology (Rhoads and Fassihi, 2011). Implementing the Network has been costly for the government, too (Millichronicle, 2020, Freedom House, 2018).

Additionally, mobile operators in Iran have lost the equivalent of millions of dollars due to the country's policy of "filtering," or restricting, Internet access (Salami, 2023). To bypass some of these restrictions, many Iranians purchase virtual private networks (VPNs), which can help them access blocked websites, including social media (Dehghan, 2012; Castro, 2024). Sales of VPNs generate millions of dollars, but VPN providers are not taxed–so these sales do not economically benefit the Iranian government (Salami, 2023).

Furthermore, this blocking is largely specific to ICTs. During the same recent period, Iran's approach to other technologies and sectors has resembled the facilitative side of investment. And these economic investments are also likely influenced by the government, as the economy is largely controlled by the state (CIA, n.d.). Overall, Iran's import levels are comparable to other countries in the region. Iranians also have robust access to electricity, and energy consumption per capita is middling compared to its neighbors; additionally, Iran has more transportation infrastructure than most Middle Eastern nations (CIA, n.d.). Finally, Iran ranks highly compared to other middle income countries on the Global Innovation Index (GII, 2022; GII, 2023).

6.3 Does Blocking Follow the Model's Logic?

I now seek to establish that the logic used by Iran when blocking ICTs is consistent with the hybrid mechanism. To do this, I revisit the main questions (from Section 6) about what I expect players to do in the equilibrium.

When the Iranian government has an investment opportunity relating to ICTs, do they consider the threat of international covert influence when making their investment decision, or solely domestic or international opportunities and pressures?

This question describes the core logic of underinvestment to avoid foreign influence and unrest. The fear that foreign influence will increase domestic unrest confirms that a case of ICT underinvestment is the result of both internal and external threats. Without evidence of this logic, we wouldn't know if a state underinvested to prevent covert influence and domestic unrest, or only the latter (which would be the domestic backwardness mechanism).

While it is difficult to glean the full intentions behind any government's policy decisions, Iran being no exception, there is evidence that the threat of foreign influence factors into Tehran's motivation for blocking ICTs. Further, other instances of covert influence likely give Iranian officials reason to be concerned about foreign influence via ICTs, even if they do not publicly say so.

Iranian leaders publicly signal foreign threats when discussing ICTs, often broadly characterizing the Internet as a weapon controlled by the West and used against Iranians (Anderson, 2016; Haghighatnejad, 2016). These officials have also connected foreign threats to domestic protests. Further, Iran's leaders often describe the country as being in a "soft war" against Western influence online, and see the Internet as the primary way for adversaries to fight them (Rhoads and Fassihi, 2011).

Amid protests in 2010, Iran's Supreme Leader Khamenei claimed that the US planned to undermine Iran's government by staging "riots" (Derakhshi, 2010). In 2022, to make the case for additional restrictions on international Internet sources, Khamenei once again described the US as using social media as a weapon against Iran (Isfahani, 2022; Yee, 2022). Iran's president also accused the US of being responsible for public unrest during the 2022 protests (Gambrell, 2022), while other officials accused the West of interfering with Iranian politics (Axios, 2022). In 2023, an Iranian security official asserted that the US used popular Internet platforms for political influence against other countries (Iran International, 2023a).

These leaders' statements suggest that Tehran's perception is that ICTs contribute to covert foreign influence toward the Iranian public. A possible source of this sentiment is that US policymakers do see the Internet as a way to encourage free expression and dissent in other countries with Internet restrictions (Lum and Figliola, 2012; Glanz and Markoff, 2011). And as previously mentioned, the US has long tried to help Iranians avoid government censorship, and these efforts likely inform Tehran's concern for covert influence (for example, Khamenei's 2010 comments alluded to a US Senate bill to combat Internet restrictions in Iran) (Derakhshi, 2010).

Does the security threat to Iran posed by an adversary include the threat of covert influence, and could ICTs improve the efficacy of these operations at influencing the Iranian public?

Section 6.1 demonstrated that the United States has used covert operations against Iran. Here are several examples that further support the potential for US covert influence using ICTs.

The US has invested in projects to provide Internet access and other digital communication systems to dissenters in countries with restrictions on technology, including Iran (Glanz and Markoff, 2011; Clinton, 2011). And, although not a covert operation, during protests over Iran's disputed 2009 election, the US Department of State asked Twitter to postpone a scheduled system upgrade that would have temporarily blocked access to the platform for Iranians (Pleming, 2009). The State Department has also looked for ways to help Iranians bypass Internet blockages during recent protests (Kaviani, 2022). In response to additional Internet shutdowns in 2022, the Treasury Department recommended modifying sanctions against Iran to allow Iranians to better resist censorship, and allowed technology companies to improve Internet access in Iran (Psaledakis et al., 2022; Polglase et al., 2022; Hussein, 2022). These events demonstrate US policymakers' considerations of the use of ICTs for communication and coordination in Iran, and could support covert policies that aim to assist protest movements.

More broadly, unconcealed foreign influences enabled by ICTs may also support the US's goals against Iran. Researchers argue that the Internet's capability for global communication gave protesters international support against the Iranian government during the Green Movement in 2009, while ICTs also improved domestic organization against the regime (Sohrabi-Haghighat and Mansouri, 2010). Removing current ICT restrictions (which focus on international web content) would likely expand Iranians' exposure to international media and facilitate global communication, increasing that international support in the event of a protest or opposition movement (Tajdin, 2013).

If Iran allowed more open access to the global Internet and other ICTs, the US would likely have more opportunities to influence the Iranian public and support dissenters. Research suggests that the US covertly uses social media accounts to criticize its foreign adversaries and encourage pro-Western content, focusing its influence on users in Asia and the Middle East, including Iran. In fact, this activity uses similar digital strategies to recent election influence by Russia and China against the US (Graphika, 2022). Without filtering of social media platforms, more Iranians could be exposed to messages from these operations. Opening ICT access would also help achieve the US's overt goals of facilitating free communication and expression online (Kaviani, 2022).

In summary, Iran's government has signaled that the concern of foreign political influence motivates their policies of restricting Internet access. And, expanding Internet access would likely support the United States' foreign policy goals in Iran by giving Iranians more exposure to US influence, which could encourage dissenters during times of public unrest.

6.4 Potential Deviant Cases: What Motivated Iran's Facilitative ICT Policies?

As Table 1 shows, Iran has not blocked ICTs at every opportunity. Rather, especially early on in the 1990s, they have facilitated ICTs. Specifically, Iran mostly welcomed Internet access and allowed (but regulated) private-sector ISPs (Rhoads and Fassihi, 2011; Miller et al., 2023). At first, this seems inconsistent with my theory. The US was still a powerful adversary, and potential covert threat, at this time. What explains these cases of ICT investment?

I argue that, while the threat environment may have been the same, Iran's concerns about the effects of ICTs in the 1990s were different. This early era likely represents a period when ICTs had a smaller effect on the capacity for foreign covert influence. ICTs were not as globally widespread, and the Internet was not as internationally connected or accessible as it would become (World Bank, n.d.; OECD, n.d.-b). So it is probable that at this time, governments were less concerned about covert influence in general, and instead held the economic and domestic benefits of ICTs at the center of their motivation to invest.

This suggests that only later on in the Internet's development did this case contain the preconditions for hybrid underinvestment. Although I did not plan to see this when coding Iran's ICT policies, it makes intuitive sense that in their early days, when they are still being implemented worldwide, ICTs are less consequential for security concerns (particularly covert influence) and thus we are less likely to see hybrid blocking.

Additionally, Table 1 lists facilitative policies that have continued past the dawn of the Internet in Iran. These policies may also seem inconsistent with my theory, but I argue that they involve ICTs with less of an effect on covert influence, putting them outside the scope of the hybrid underinvestment equilibrium. According to my mechanistic predictions, states adhering to the equilibrium strategy should only block ICTs that would enable foreign influence on domestic unrest. So, they may still facilitate ICTs that do not have this effect.

One such facilitative policy is Iran's importation of computers and media devices, along with its encouragement of domestic technology production. These actions are facilitative, but they likely impact aspects of ICTs that are less relevant for covert influence. Namely, access to Internet hardware on its own does not create the conditions for foreign online influence. Despite continuing attempts to improve Internet access overall and reduce costs, Iran heavily regulates how Iranians can use that access (Freedom House, 2018). This fact is consistent with the mechanistic hypothesis that Iran directs its blocking policies at types and uses of ICTs that would enable foreign influence.

Additionally, Iran's government has set goals to improve ICT access and innovation in its Five-Year Development Plans (see Appendix A.2 for details). While these official policies are efforts to facilitate ICTs, they seem to primarily aim to improve Internet penetration overall and make the Iranian economy more dependent on "knowledge" industries (UNCTAD, 2005; Amuzegar, 2010; Amiri and Sangar, 2023; Bakhtiari, 2021). They do not preclude the government's restrictions on ICT use, and some specifically encourage the National Information Network, Iran's domestic alternative to the Internet which only provides access to approved online sites (Bakhtiari, 2021).

6.5 Concerns and Alternative Explanations

6.5.1 Concerns

The Existence of Overt Conflicts by the US against Iran: This paper is primarily interested in covert operations designed to effect regime change. Outside of this context are instances in which the United States overtly strikes or meddles against Iran (also mentioned in Section 6.1). However, these operations are not designed to overthrow Iran's government; rather, they often target specific military figures and are often reactive to particular military actions by Iran. Because of their lower-level scale, these instances are somewhat outside the scope of the model's interpretation of overt intervention.

Unequal Benefit of ICTs for the Regime and Public: Overall, restricting the Internet has prevented Iranians from obtaining the benefits of more and better Internet access. However, government officials and other elites have been allowed some of those benefits anyway. For example, many government officials have accounts on social media platforms banned for most Iranians (Majidyar, 2018; Toor, 2013; Torbati, 2012; Kenyon, 2013; Yee, 2022). Unlike most Iranians, foreign tourists and Iranian employees of travel agencies are allowed full internet access (Iran International, 2023b). Iran has also implemented policies in which certain groups, such as journalists, schools, and businesses, can access some of the online content Iran otherwise filters (Seifi, 2023; Akbarpour, 2022).

In the models, one could reflect this observation by allowing T to get part of the benefit of innovating (α), even if it blocks ICTs overall ($z = 0$) and prevents M from getting any α. The current extended model cannot account for this, but doing so would likely create wider conditions for hybrid blocking. Why? Currently, if α is large enough to outweigh the costs of domestic unrest, T facilitates ICTs. If T could obtain part of α regardless of whether it facilitates, α would have to be even higher to deter blocking (if the other conditions that produce hybrid blocking are met).

Additionally, the implementation of some ICT restrictions, like the National Information Network, have been costly for the Iranian government (Freedom House, 2018; Millichronicle, 2020), whereas in the model, T incurs no added cost to blocking ICTs besides the opportunity cost of ICT benefits (α). The fact that the government was willing to pay these costs to restrict ICTs, however, demonstrates a strong incentive to block ICTs consistent with the hybrid blocking mechanism.

6.5.2 Alternative Explanations

There are other compelling depictions of the mechanism that led Iran to underinvest in ICTs. For example, some scholars might argue that Iran's ICT policies are better explained with our current understanding of domestically-induced economic backwardness, where a government blocks technology to avoid the domestic threat of unrest and foreign threats only discourage blocking. This explanation is mostly convincing, but it is unlikely comprehensive. My theory could explain some of the empirical phenomenon that alternative explanations like this cannot.

One other explanation for Iran's ICT policies is that despite public statements, the regime limits ICT access *only* because of their potential to better organize existing domestic opposition, not because they might allow foreign adversaries to influence domestic opposition. If this were the case, Iran would represent a case of domestically induced, not hybrid, underinvestment.

However, rather than blocking ICT access overall, Iran's policies focus on blocking aspects of ICTs that involve foreign influence, while allowing other types of ICTs. For instance, Iran's National Information Network aims to provide advantages of an Internet–including improved communication and research opportunities–while cutting Iranians off from online sources, many of them external, that oppose regime's ideals or encourage reforms (Tajdin, 2013). Additionally, public officials explicitly suggest that concerns about foreign influence drive Iranian leaders' support for blocking policies (Anderson, 2016; Haghighatnejad, 2016; Rhoads and Fassihi, 2011). And, while shutting down certain social media platforms during periods of unrest exemplifies blocking to suppress existing domestic opposition, even these actions also block access to international communication that could influence protests.

A second counterargument is that Iran's government always wanted to restrict ICTs but did not, because they wanted to avoid public opposition. Then, when foreign threats increased, Iran could hope for more public support for ICT restrictions by portraying them as a way to resist foreign influence. If this explanation were the case, ICT restrictions would represent domestic blocking.

Contrary to this counterargument, scholars argue that Iranian officials are privately concerned that ICTs are a tool for foreign influence, in addition to their public statements making the same claim (Enayat, in Rhoads and Fassihi, 2011). Iran's own online influence operations against the US also suggest that Iran's leaders want to deter similar operations against themselves (Grzegorzewski et al., 2022). Further, Iran's domestic Internet disproportionately blocks Western websites and platforms, a sign that foreign influence concerns drive official policy (Brooking and Kianpour, 2020).

This counterargument also conflicts with the fact that Iran began expanding its ICT capabilities faster than neighboring countries. If Iran's ICT growth matched neighboring countries, public opposition would not likely amass. Iran has also not needed foreign influence concerns to justify Internet restrictions. After reformist journalists established a popular domestic online community in the early 2000s, the government responded by blocking thousands of websites (Rhoads and Fassihi, 2011).

Moreover, if this explanation were the case, we might not see Iran taking steps to improve its domestic Internet. Instead, Iran's government has introduced policies to improve bandwidth and online business (Rezaian, 2023). It has also tried to popularize its own social media apps (although unsuccessfully) (MacLellan, 2018).

Another counterargument is that Iran mainly blocks ICTs to deter foreign cyberattacks, like Stuxnet, rather than foreign influence operations that involve the domestic public. For instance, after Stuxnet was exposed, Iran took additional steps to prevent further attacks and retaliate (Shalal-Esa, 2013).

However, Iran had already been developing ICT restrictions, including its National Information Network, well before Operation Olympic Games took effect. Further, many of the domestic restrictions on ICT access, which the government claims protect against cyberattacks, do not significantly prevent experts from infiltrating Iran's domestic Internet from abroad, suggesting that the cyberattack did not lead to Iran's later ICT blocking, either (Tajdin, 2013).

If true, this counterargument would still be an example of blocking ICTs to deter foreign covert threats, although that threat would instead be cyberattacks, which do not involve the domestic population. So this possibility would represent a different type of blocking that the model cannot directly illustrate. However, the overall mechanism would be the same as for hybrid blocking–blocking ICTs to avoid increasing the efficacy of covert action by foreign adversaries.

7 Conclusion

In the international relations literature, it is often assumed that states facing foreign threats–particularly covert threats–have greater incentives to invest in technologies, including ICTs, to reduce the probability that foreign intervention occurs successfully (Joseph and Poznansky, 2018). Scholars of economic backwardness also predict that external threats discourage backwardness (Acemoglu and Robinson, 2006). In this paper, I made a theoretical argument that, in the case of modern ICTs, this assumption is not always true.

I proposed two mechanisms in which foreign threats (in particular, covert threats) encourage a target state to block Internet and communication technologies. In the first mechanism, I showed that a state may underinvest in ICTs–the very technologies that help expose foreign covert operations–to avoid creating a situation where a foreign adversary prefers overt intervention, a costlier and riskier outcome for the target state. In this mechanism, the target state blocks technologies because it *prefers* the threat of covert intervention, which is smaller scale and less likely to successfully overthrow them than an overt intervention.

In the second mechanism, I distinguished two competing effects that modern ICTs have on covert intervention: they can help detect and expose covert operations, but they can also help interveners covertly influence domestic politics. States vulnerable to this type of foreign influence may be incentivized to block ICTs that have the latter effect, in order to prevent a foreign intervener from inciting domestic unrest and endangering their regime.

These predictions may help explain modern instances of economic backwardness when the traditional domestic-politics explanation is insufficient. Specifically, the first mechanism proposes that technological underinvestment can occur without any threat of domestic unrest. The second mechanism illustrates that foreign threats can complement domestic threats, to induce underinvestment.

The second mechanism, in particular, speaks to the importance of studying modern economic backwardness in the context of both domestic and international pressures. It implies that foreign interveners, through covert influence, can create or boost domestic unrest, encouraging governments to block technologies that support foreign influence. So, if a modern case of technological backwardness seems to be caused purely by the domestic threat of unrest, my mechanism suggests that foreign threats may also contribute to the incentive to block technology. I used the case of

Iran and its Internet restrictions to demonstrate this mechanism, showing that Tehran limits ICTs, not only because of their ability to assist domestic unrest, but also because of their concern that foreign adversaries can use ICTs to influence domestic opinions toward unrest.

This explanation may apply to other modern governments that restrict Internet technologies. Since ICTs today are globally shared, the threat of foreign political influence is a likely motivation for many governments that wish to restrict ICTs.

My theory also suggested that these mechanisms could appear in democracies, too. My second novel blocking mechanism, where governments block technologies that would enable covert foreign influence on the public's political support, may be especially relevant for democracies. For example, leaders in countries like the United States are beginning to grapple with the political influence of international adversaries on social media users, and have taken actions to limit this influence. Perhaps most notable are policies to limit China's influence over political content on TikTok (Maheshwari and Holpuch, 2024). Further research could explore (1) whether such policies are inhibitory enough to actually represent ICT blocking or economic backwardness, and (2) whether the motivations behind those policies resemble a desire to limit covert foreign influence that could cause unrest.

A Appendix

A.1 Formal Appendix

Here I will write proofs for the blocking equilibria shown in the paper's propositions. I work backward in the sequence of events, using the one-shot deviation principle to show that each player's strategy has no profitable deviations, and thus forms a sub-game perfect equilibrium (Osborne, 2004).

For the equilibrium plots shown in the paper, I solve for equilibria corresponding to each region in each plot, plugging in the parameter values used to draw the plot.

Recall the formal description of players' strategies: a strategy profile for T is $s^T(z \in \{0,1\})$, where $z = 1 \implies T$ facilitated ICTs. A strategy profile for A is $s^A(a \in \{Covert,\ Overt,\ No\ Action\}|z)$.

In the extended model, a strategy profile for M is $s^M(r \in \{No\ Revolt,\ Revolt\}|z,a)$. Nature's strategy profile is $s^N(n \in \{1-p_U(z), p_U(z)|z,a\}$. If Nature chooses $p_U(z)$, covert intervention is undetected. If Nature chooses $1-p_U(z)$, covert intervention is detected.

In A.1.2, I walk through the version of the baseline model, referenced in 3.2.1, which represents ICT investment on a continuum.

A.1.1 Proof of Proposition 3.1

Working backward, following $z = 0$, A faces a terminal decision node, choosing between Covert, Overt, and No Action. A's utility from each choice is characterized as:

$$U^A(Covert|z=0) = p_C(0) - k_C$$

$$U^A(Overt|z=0) = p_O - k_O$$

$$U^A(NoAction|z=0) = 0$$

The equilibrium conditions are derived for solving where Covert is the best response over the others. Specifically, $p_C(0) - k_C \geq p_O - k_O \geq 0$. Thus, A cannot increase its payoff by deviating to Overt or No Action.

Similarly, if $z = 1$,

$$U^A(Covert|z=1) = p_C(1) - k_C$$

$$U^A(Overt|z=1) = p_O - k_O$$

$$U^A(NoAction|z=1) = 0$$

The equilibrium conditions are derived from solving where Overt is the best response over the others. Specifically, $p_O - k_O \geq p_C(1) - k_C, 0$. Thus, A cannot increase its payoff by deviating to Covert or No Action.

This covers A's decision nodes. At the initial node, T faces the choice between $z = 0$ and $z = 1$.

Knowing what A is going to do, T's utility from each choice is characterized as:

$$U^T(z = 0) = 1 - p_C(0)$$

$$U^T(z = 1) = (1 + \alpha)(1 - p_O)$$

The equilibrium conditions are derived from solving where $z = 0$ is the best response, over $z = 1$. Specifically, $1 - p_C(0) \geq (1 + \alpha)(1 - p_O)$. Thus, T cannot increase its payoff by deviating to $z = 1$.

This is the only equilibrium in which T plays $z = 0$. If $p_O - k_O > p_C(0) - k_C, 0$, A would always play Overt. If $0 > p_O - k_O, p_C(0) - k_C$, A would always play No Action. If $p_C(0) - k_C > p_C(1) - k_C > p_O - k_O, 0$ (and $p_C(0) - k_C > p_C(1) - k_C$ always), A would always play Covert. As mentioned before, when T faces the same outcome with or without ICTs, it facilitates them. Finally, if $1 - p_C(0) < (1 + \alpha)(1 - p_O)$, T would face Covert if $z = 0$ and Overt if $z = 1$, but it would prefer to facilitate ICTs and face Overt.

A.1.2 Baseline Model 2 (Robustness Check)

In this section, I modify the initial model by making z a continuous variable that can be set to any value from 0 to 1, rather than a variable that can be set only at 0 or 1. This more specifically illustrates the extent to which the target state invests in ICTs.

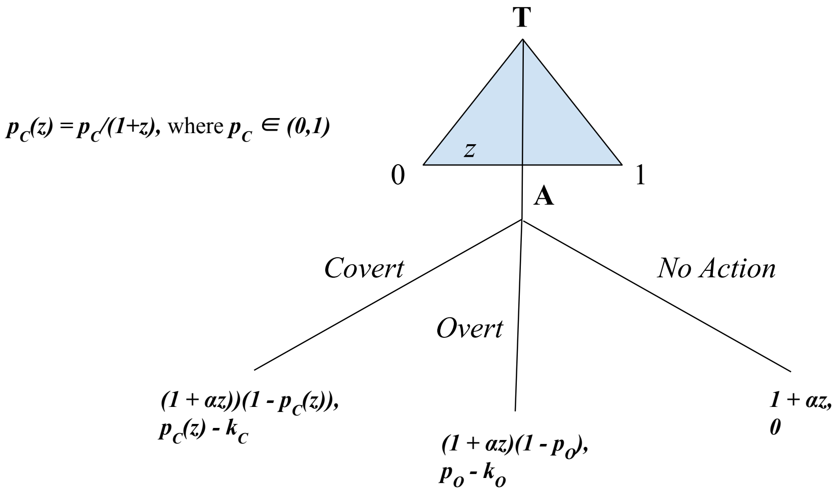

T
$p_C(z) = p_C/(1+z)$, where $p_C \in (0,1)$
z
0
1
A
Covert
Overt
No Action
$(1 + \alpha z))(1 - p_C(z))$,
$p_C(z) - k_C$
$(1 + \alpha z)(1 - p_O)$,
$p_O - k_O$
$1 + \alpha z$,
0

Figure 8: Game Tree for the Baseline Model version 2

Here, T's benefit from facilitating ICTs is αz, a positive number that increases as more investment occurs. T gets no additional utility when it does not invest at all.

Also, $p_C(z) = \frac{p_C}{1+z}$, where the constant $p_C \in (0, 1)$ represents the probability of successful covert action when there is no investment (so $p_C(0) = p_C$). The equation means that the probability of successful covert action decreases as investment in the target state increases. So, like the initial model, $p_C(0) > p_C(1)$. The game tree and payoffs are shown in Figure 2.

A.1.3 Baseline Model 2 Analysis

Economic backwardness, or underinvestment, occurs when T sets z at any level below 1, since its payoff increases with z, holding constant A's action. In this model, there are conditions that produce backwardness, and these conditions are very similar to those that produce backwardness in Baseline Model 1.

Proposition A.1 *If*

$$p_C(0) - k_C \geq p_O - k_O \geq 0, p_C(1) - k_C;$$

$$0 \leq \frac{p_C}{k_C + p_O - k_O} - 1 < 1; \textit{ and}$$

$$(1 + \alpha(z))(1 - p_C(z)) \geq (1 + \alpha(1))(1 - p_O)$$

then the following strategies are sub-game perfect. T sets $z = \frac{p_C}{k_C+p_O-k_O} - 1$, which is below the maximum level of $z = 1$. A plays Covert if $z \leq \frac{p_C}{k_C+p_O-k_O} - 1$ and would play Overt if $z > \frac{p_C}{k_C+p_O-k_O} - 1$.

So, T invests only partially to prevent A from moving from covert to overt intervention. T sets z so to the highest level for which A will conduct Covert intervention, or when $p_C(z) - k_C = p_O - k_O$. Plugging this into the proposition's third inequality, we get:

$$(1 + \alpha(\frac{p_C}{k_C + p_O - k_O} - 1))(1 - k_C - p_O + k_O) \geq (1 + \alpha(1))(1 - p_O)$$

If this is true, underinvesting is a best response for T.

Proof for Proposition A.1:

Following $z = \frac{p_C}{k_C+p_O-k_O} - 1$, A's utility from each choice can be characterized by:

$$U^A(Covert|z = \frac{p_C}{k_C + p_O - k_O} - 1) = p_C(\frac{p_C}{k_C + p_O - k_O} - 1) - k_C$$

$$U^A(Overt|z = \frac{p_C}{k_C + p_O - k_O} - 1) = p_O - k_O$$

$$U^A(NoAction|z = \frac{p_C}{k_C + p_O - k_O} - 1) = 0$$

The proposition's equilibrium conditions are derived from solving where Covert is a best response over the others. Specifically, $p_C(\frac{p_C}{k_C+p_O-k_O} - 1) - k_C = p_O - k_O \geq 0$. Thus, A cannot increase its payoff by deviating to Overt or No Action.

When $z < \frac{p_C}{k_C+p_O-k_O} - 1$, A's utility from each choice can be characterized by:

$$U^A(Covert|z = \frac{p_C}{k_C + p_O - k_O} - 1) = p_C(z) - k_C$$

$$U^A(Overt|z = \frac{p_C}{k_C + p_O - k_O} - 1) = p_O - k_O$$

$$U^A(NoAction|z = \frac{p_C}{k_C + p_O - k_O} - 1) = 0$$

The proposition's equilibrium conditions are derived from solving where Covert is a best response over the others. Specifically, $p_C(z) - k_C > p_O - k_O, 0$ for $z < \frac{p_C}{k_C+p_O-k_O} - 1$. Thus, A cannot increase its payoff by deviating to Overt or No Action.

Similarly, if $z > \frac{p_C}{k_C+p_O-k_O} - 1$:

$$U^A(Covert|z = \frac{p_C}{k_C + p_O - k_O} - 1) = p_C(z) - k_C$$

$$U^A(Overt|z = \frac{p_C}{k_C + p_O - k_O} - 1) = p_O - k_O$$

$$U^A(NoAction|z = \frac{p_C}{k_C + p_O - k_O} - 1) = 0$$

The proposition's equilibrium conditions are derived from solving where Overt is a best response over the others. Specifically, $p_O - k_O > p_C(z) - k_C, 0$ for $z > \frac{p_C}{k_C+p_O-k_O} - 1$. Thus, A cannot increase its payoff by deviating to Covert or No Action.

That covers A's decision node. At the initial node, T can set z to any level between 0 and 1. Knowing what A is going to do, T's utility function can be characterized as:

$$U^T(z \leq \frac{p_C}{k_C + p_O - k_O} - 1) = (1 + \alpha(z))(1 - p_C(z))$$

$$U^T(z > \frac{p_C}{k_C + p_O - k_O} - 1) = (1 + \alpha(z))(1 - p_O)$$

which each increase with z.

The proposition's equilibrium conditions are derived from solving where $z = \frac{p_C}{k_C+p_O-k_O} - 1$ is a best response to all other z values. Specifically, any value lower than that would still induce covert intervention (with a higher probability of remaining undetected) and give T a smaller $\alpha(z)$. Any higher value of z would induce overt intervention, and T's payoff would increase with z; however even at $z = 1$, the highest level:

$$(1 + \alpha(\frac{p_C}{k_C + p_O - k_O} - 1))(1 - p_C(\frac{p_C}{k_C + p_O - k_O} - 1)) \geq (1 - \alpha(1))(1 - p_O)$$

So it is no better to set $z = 1$ and induce overt intervention than to set $z = \frac{p_C}{k_C+p_O-k_O} - 1$ and induce covert intervention. Thus, T cannot increase its payoff by setting z any higher or lower.

The above equilibrium conditions can be satisfied with the following values of p_O, k_O, $p_C(0)$, and k_C:

$$p_O = 0.7, k_O = 0.5, p_C(0) = 0.4 \text{ and } k_C = 0.1$$

These values conform to the other assumptions in the game, namely: $p_O > p_C(0) > p_C(z) > p_C(1)$ and $k_O > k_C$. They also produce backwardness in the baseline model. Solving the inequalities for the remaining values (α and $\frac{p_C}{k_C+p_O-k_O} - 1$–the value of z for which A switches from covert to overt intervention if $p_O - k_O > 0$) yield:

$$z = \frac{p_C}{k_C + p_O - k_O} - 1 = 0.3 \text{ and } \alpha < 6$$

These values satisfy the game's conditions, $z \in [0,1]$ and $\alpha > 0$. T's z value also satisfies the equilibrium condition $0 \leq \frac{p_C}{k_C + p_O - k_O} - 1 < 1$. (If $z = 1$, T would be innovating fully, so in the blocking equilibrium $0 \leq z < 1$ must hold.)

A.1.4 Extended Model Proofs: Conditions under which M revolts

In Section 5.1, I isolated the conditions under which trying to replace T (revolting) is a best response for M, at each of its decision nodes. Recall:

When: (subgame)	M revolts if...
T blocks ICTs and A plays No Action	$b \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$ (C1)
T blocks ICTs and A plays Covert and is undetected	$b(1 - p_E(0)) \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$ (C2)
T facilitates ICTs and A plays No Action	$b \leq \frac{1}{2}(1 - \frac{w_1}{p_R})$ (C3)
T facilitates ICTs and A plays Covert and is undetected	$b(1 - p_E(1)) \leq \frac{1}{2}(1 - \frac{w_1}{p_R})$ (C4)

The above conditions are found by solving where Revolt is M's best response, at each of its four decision nodes.

If T blocked ICTs and A played No Action, M's utility from each choice is characterized by the following:

$$U^M(\mathit{NoRevolt}|z = 0, a = \mathit{NoAction}) = b$$

$$U^M(\mathit{Revolt}|z = 0, a = \mathit{NoAction}) = (1 - b + \alpha)p_R + b(1 - p_R) - w_0$$

For Revolt to be a best response,

$$b \leq (1 - b + \alpha)p_R + b(1 - p_R) - w_0 \tag{C1}$$

This simplifies to $b \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$, which is condition C1.

If T blocked ICTs and A played Covert action undetected, M's utility from each choice is characterized by the following:

$$U^M(\mathit{NoRevolt}|z = 0, a = \mathit{Covert}, n = p_U(0)) = b(1 - p_E(0))$$

$$U^M(\mathit{Revolt}|z = 0, a = \mathit{Covert}, n = p_U(0)) = 1 - b(1 - p_E(0)) + \alpha]p_R + b(1 - p_E(0))(1 - p_R) - w_0$$

For Revolt to be a best response,

$$b(1 - p_E(0)) \leq 1 - b(1 - p_E(0)) + \alpha]p_R + b(1 - p_E(0))(1 - p_R) - w_0 \tag{C2}$$

This simplifies to $b(1 - p_E(0)) \leq \frac{1}{2}(1 + \alpha - \frac{w_0}{p_R})$, which is condition C2.

If T facilitated ICTs and A played No Action, M's utility from each choice is characterized by the following:

$$U^M(\mathit{NoRevolt}|z = 1, a = \mathit{NoAction}) = b + \alpha$$

$$U^M(\mathit{Revolt}|z = 1, a = \mathit{NoAction}) = (1 - b)p_R + b(1 - p_R) + \alpha - w_1$$

For Revolt to be a best response,

$$b + \alpha \leq (1-b)p_R + b(1-p_R) + \alpha - w_1 \tag{C3}$$

This simplifies to $b \leq \frac{1}{2}(1 - \frac{w_1}{p_R})$, which is condition C3.

If T facilitated ICTs and A played Covert action undetected, M's utility from each choice is characterized by the following:

$$U^M(NoRevolt|z=1, a=Covert, n=p_U(1)) = b(1-p_E(1)) + \alpha$$

$$U^M(Revolt|z=1, a=Covert, n=p_U(1)) = [1-b(1-p_E(1))]p_R + b(1-p_E(1))(1-p_R) + \alpha - w_1$$

For Revolt to be a best response,

$$b(1-p_E(1)) + \alpha \leq [1-b(1-p_E(1))]p_R + b(1-p_E(1))(1-p_R) + \alpha - w_1 \tag{C4}$$

This simplifies to $b(1-p_E(1)) \leq \frac{1}{2}(1-\frac{w_1}{p_R})$, which is condition C4.

A.1.5 Underinvestment in ICTs to avoid domestic unrest

In the main text, I explained that the extended model supports five equilibria where T blocks ICTs to avoid domestic revolt. In some of these, T blocks ICTs and faces no foreign intervention. In others, T blocks ICTs and tolerates overt intervention. Here I describe one of the former types, which most clearly illustrates underinvestment as a result of domestic pressure. I call this equilibrium D1.

> **Proposition A.2** *Suppose C3 and C4 hold. If $p_O - k_O \leq 0$ and $1 \geq (1+\alpha)(1-p_R)$, the following strategy is sub-game perfect. T blocks ICTs. A selects No Action regardless of whether T blocked or facilitated ICTs. M revolts if T facilitated ICTs and regardless of whether A played Covert intervention (i.e. if $a \in \{Covert, NoAction\}$). Otherwise, M does not revolt.*
>
> *On the path, we observe ICT underinvestment, no foreign intervention, and no domestic revolt. Off the path ($z=1$), we would observe no foreign intervention and domestic revolt.*

Proof of Proposition A.2

Working backward, we start with M. Since C3 and C4 hold, Revolt is a best response when $z=1$ and No Revolt is a best response when $z=0$, regardless of whether A has covertly intervened.

Now consider A's decision nodes. Knowing what M will play, when $z=0$, A's utility from each action is characterized by:

$$U^A(Covert|z=0) = -k_C$$

$$U^A(Overt|z=0) = p_O - k_O$$

$$U^A(NoAction|z=0) = 0$$

The equilibrium conditions are derived from solving where No Action is a best response over the others. Specifically, $0 > -k_C$ and $0 \geq p_O - k_O$. So, A cannot increase its payoff by deviating to

Covert or Overt.

Similarly, if $z = 1$:

$$U^A(Covert|z = 1) = p_U(1)p_R - k_C$$
$$U^A(Overt|z = 1) = p_O - k_O$$
$$U^A(NoAction|z = 1) = p_R$$

The equilibrium conditions are derived from solving where No Action is a best response over the others. Specifically, $p_R \geq p_O - k_O$ and $p_R > p_U(1)p_R - k_C$.

This covers A's decision nodes. At the initial node, knowing what A and M will play, T's utility from each of its choices is characterized by:

$$U^T(z = 0) = 1$$

$$U^T(z = 1) = (1 + \alpha)(1 - p_R)$$

The equilibrium conditions are derived from solving where $z = 0$ is a best response over $z = 1$. Specifically, $1 \geq (1 + \alpha)(1 - p_R)$. Thus, T cannot increase its payoff by deviating to $z = 1$.

Also reachable in the model are domestic blocking equilibria D2, D3, D4, and D5. D3 has the same outcome as D1. In D2, D4, and D5, T still blocks ICTs to avoid domestic unrest, but it tolerates Overt intervention or Covert influence by doing so. Acemoglu and Robinson argued that external threats always encourage innovation rather than blocking, which these equilibria may seem to contradict. However, equilibria D2, D3, and D5 are really instances of T being extremely afraid of domestic unrest, so much so that it would rather face Overt or Covert intervention without innovation. So these particular equilibria could be seen as extreme examples of Acemoglu and Robinson's blocking mechanism.

A.1.6 Underinvestment in ICTs to avoid overt intervention (external underinvestment)

In the main text, I explained that the extended model supports four equilibria where T blocks ICTs to avoid overt intervention. In two of these equilibria (called E2 and E3), T blocks ICTs and tolerates covert intervention, which could cause domestic unrest. Here I describe E2.

> **Proposition A.3** *Suppose C2 holds. If $p_U(0)p_R - k_C \geq p_O - k_O \geq 0$ and $1 - p_U(0)p_R \geq (1+\alpha)(1 - p_O)$, the following strategies are sub-game perfect. T blocks ICTs. A selects Covert intervention if T blocked and Overt if T facilitated. M revolts if T blocked and A conducted Covert intervention undetected. Otherwise, M does not revolt.*
>
> *On the path, we observe ICT underinvestment, covert intervention, and possible domestic unrest. Off the path ($z = 1$), we would observe investment and overt intervention.*

Proof of Proposition A.3

Working backward, we start with M. Since C2 holds, Revolt is a best response when $z = 0$ and A covertly intervenes successfully (i.e. $a = Covert$ and Nature chooses $p_U(0)$). Otherwise, No Revolt is the best response.

Now consider A's decision nodes. Knowing what M will play, when $z = 0$, A's utility from each action is characterized by:

$$U^A(Covert|z = 0) = p_U(0)p_R - k_C$$

$$U^A(Overt|z = 0) = p_O - k_O$$

$$U^A(NoAction|z = 0) = 0$$

The equilibrium conditions are derived from solving where Covert is a best response over the others. Specifically, $p_U(0)p_R - k_C \geq p_O - k_O, 0$. Thus, A cannot increase its payoff by deviating to Overt or No Action.

Similarly, if $z = 1$:

$$U^A(Covert|z = 1) = -k_C$$

$$U^A(Overt|z = 1) = p_O - k_O$$

$$U^A(NoAction|z = 1) = 0$$

The equilibrium conditions are derived from solving where Overt is a best response over the others. Specifically, $p_O - k_O \geq 0 > -k_C$. Thus, A cannot increase its payoff by deviating to Covert or No Action.

This covers A's decision nodes. At the initial node, knowing what A and M will play, T's utility from each of its choices is characterized by:

$$U^T(z = 0) = 1 - p_U(0)p_R$$

$$U^T(z = 1) = (1 + \alpha)(1 - p_O)$$

The equilibrium conditions are derived from solving where $z = 0$ is a best response over $z = 1$. Specifically, $1 - p_U(0)p_R \geq (1 + \alpha)(1 - p_O)$. Thus, T cannot increase its payoff by deviating to $z = 1$.

The mechanism of E2 also occurs in a different equilibrium, E3. The only difference is that in E3, C2 and C4 hold, so M would also revolt if $z = 1$, $a = Covert$, and $n = p_U(1)$. However, under E3's conditions, A still prefers to conduct overt intervention when $z = 1$, so the external blocking mechanism from E2 remains.

In the other two equilibria where T blocks ICTs to avoid overt intervention (E1 and E4), T blocks ICTs and tolerates domestic unrest, rather than covert intervention that can lead to unrest. Here I describe E1.

Proposition A.4 *Suppose C1 and C2 hold. If $p_R \geq p_O - k_O \geq 0$ and $1 - p_R \geq (1 + \alpha)(1 - p_O)$, the following strategies are sub-game perfect. T blocks ICTs. A selects No Action if T blocked and Overt intervention if T facilitated. M revolts if T blocked, regardless of whether A played Covert intervention (i.e. if $a \in \{Covert, NoAction\}$).*

On the path, we observe ICT underinvestment, no foreign intervention, and domestic revolt. Off the path ($z = 1$), we would observe ICT investment and Overt intervention.

Proof of Proposition A.4

Working backward, we start with M. Since C1 and C2 hold, Revolt is a best response when $z = 0$

and No Revolt is a best response when $z = 1$, regardless of whether A has covertly intervened successfully or played No Action.

Now consider A's decision nodes. Knowing what M will play, when $z = 0$, A's utility from each action is characterized by:

$$U^A(Covert|z = 0) = p_U(0)p_R - k_C$$

$$U^A(Overt|z = 0) = p_O - k_O$$

$$U^A(NoAction|z = 0) = p_R$$

The proposition's equilibrium conditions are derived from solving where No Action is the best response over the others. Specifically, $p_R \geq p_O - k_O$ and $p_R > p_U(1)p_R - k_C$. Thus, A cannot increase its payoff by deviating to Covert or Overt.

Similarly, if $z = 1$:

$$U^A(Covert|z = 1) = -k_C$$

$$U^A(Overt|z = 1) = p_O - k_O$$

$$U^A(NoAction|z = 1) = 0$$

The proposition's equilibrium conditions are derived from solving where Overt is the best response over the others. Specifically, $p_O - k_O \geq 0 > -k_C$. Thus, A cannot increase its payoff by deviating to Covert or No Action.

This covers A's decision nodes. At the initial node, knowing what A and M will play, T's utility from each of its choices is characterized by:

$$U^T(z = 0) = 1 - p_R$$

$$U^T(z = 1) = (1 + \alpha)(1 - p_O)$$

The equilibrium conditions are derived from solving where $z = 0$ is a best response over $z = 1$. Specifically, $1 - p_R \geq (1 + \alpha)(1 - p_O)$. Thus, T cannot increase its payoff by deviating to $z = 1$.

The mechanism of E1 also occurs in a different equilibrium, E4. The only difference is that, in E4, C1. C2, and C4 hold, so M would also revolt if $z = 1$, $a = Covert$, and $n = p_U(1)$. However, under E4's conditions, A still prefers to conduct overt intervention when $z = 1$, so the external blocking mechanism from E1 remains.

A.1.7 Proof of Proposition 4.1 (underinvestment in ICTs to avoid covert, foreign influenced unrest; hybrid underinvestment)

Working backward, we start with M. Since C4 holds, Revolt is a best response when $z = 1$ and A covertly intervenes successfully(i.e. $a = Covert$ and Nature plays $p_U(1)$). Otherwise, No Revolt is a best response.

Now consider A's decision nodes. Knowing what M will play, when $z = 0$, A's utility from each action is characterized by:

$$U^A(Covert|z = 0) = -k_C$$

$$U^A(Overt|z = 0) = p_O - k_O$$

$$U^A(NoAction|z=0) = 0$$

The proposition's equilibrium conditions are derived from solving where No Action is a best response. Specifically, $0 \geq p_O - k_O$ and $0 > -k_C$. Thus, A cannot increase its payoff by deviating to Covert or Overt.

Similarly, when $z = 1$:

$$U^A(Covert|z=1) = p_U(1)p_R - k_C$$

$$U^A(Overt|z=1) = p_O - k_O$$

$$U^A(NoAction|z=1) = 0$$

The proposition's equilibrium conditions are derived from solving where Covert is a best response. Specifically, $p_U(1)p_R - k_C \geq p_O - k_O, 0$. Thus, A cannot increase its payoff by deviating to Overt or No Action.

This covers A's decision nodes. At the initial node, knowing what A and M will play, T's utility from each of its choices is characterized by:

$$U^T(z=0) = 1$$

$$U^T(z=1) = (1+\alpha)(1 - p_U(1)p_R)$$

The proposition's equilibrium conditions are derived from solving where $z = 0$ is a best response. Specifically, $1 \geq (1+\alpha)(1 - p_U(1)p_R)$. Thus, T cannot increase its payoff by deviating to $z = 1$.

As mentioned in the main text, proposition 4.1 represents blocking equilibrium Hy1. The model supports another hybrid blocking equilibrium, Hy2. Hy2 is similar to Hy1, except when T blocks ICTs, A prefers Overt intervention, instead of No Action. Under Hy2's conditions, T prefers to block ICTs and face overt intervention than to facilitate ICTs and face possible covertly influenced revolt. This equilibrium requires that p_O be very low compared to $p_U(1)p_R$, and/or that α be very low.

A.1.8 Underinvestment when the model represents a democracy

When we assume that $p_R = 1$ and $w_0 = w_1 = 0$, we can create the conditions under which voting T out of office is a best response for M. I do this by plugging those values into the conditions under which M revolts (C1-C4), creating new conditions C1'-C4'.

When (subgame)	M votes T out if...	
T blocks ICTs and A plays No Action	$b \leq \frac{1}{2}(1+\alpha)$	(C1')
T blocks ICTs and A plays Covert and is undetected	$b(1 - p_E(0)) \leq \frac{1}{2}(1+\alpha)$	(C2')
T facilitates ICTs and A plays No Action	$b \leq \frac{1}{2}$	(C3')
T facilitates ICTs and A plays Covert and is undetected	$b(1 - p_E(1)) \leq \frac{1}{2}$	(C4')

As with C1-C4, if C1' holds, so does C2', and if C3' holds, so does C4'. Now, though, if C3' holds, C1' and C2' also hold, in addition to C4'.

Since $p_R = 1$, A's payoff for covert intervention is now $p_U(z) - k_C$.

In section 4.3, I claimed that there are no domestic underinvestment equilibrium under these parameters. This means that when A would never intervene against T, regardless of ICTs (i.e. $0 \geq p_O - k_O, p_U(0) - k_C$), T always facilitates ICTs.

Under these conditions (A never intervenes), suppose neither C1' nor C3' hold, so M always reelects T. Facilitating ICTs is clearly T's best response, because it adds α to its payoff. If only C1' holds, M reelects T only if T facilitates ICTs. So facilitating here is a best response, too, because it ensures that T is reelected and adds α to T's payoff. There is no case where only C3' holds, since C1' must hold too. Finally, if both C1' and C3' hold, M votes T out regardless of ICTs, so T is indifferent between blocking and facilitating. Thus, there are no instances where the domestic blocking mechanism occurs.

However, we can see that external and hybrid underinvestment are still reachable. For instance, suppose only C2' holds and $p_U(0) - k_C \geq p_O - k_O \geq 0$. In other words, M reelects T unless T blocks ICTs and A conducts successful covert intervention. For A, Covert is a best response when $z = 0$ and Overt when $z = 1$. If $1 - p_U(0) \geq (1 + \alpha)(1 - p_O)$, blocking ICTs is a best response for T. When T blocks, it avoids overt intervention and faces covert intervention instead.

Now suppose only C4' holds and $p_U(1) - k_C \geq 0 \geq p_O - k_O$. Here, M reelects T unless T facilitated ICTs and A conducted successful covert intervention (so, ICTs enable A to covertly influence the election). For A, No Action is a best response when $z = 0$ and Covert when $z = 1$. If $1 \geq (1+\alpha)(1-p_U(1))$, blocking ICTs is a best response for T. When T blocks, it avoids facilitating ICTs that would allow A to covertly influence M; and if that covert influence went undetected, M would then elect a challenger to replace T.

A.2 Coding Iran's ICT Policies

In this section, I describe the ICT policies summarized in Table 1 and explain how they demonstrate blocking or facilitating.

In the 1990s, when the Internet expanded worldwide, Iran's government took steps to expand its technological capabilities and encourage Internet use. In the early 1990s, Iran was one of the first countries in its region to "go online," and its government encouraged Internet use for innovation and research, allowing private Internet service providers to open and operate in the country (Rhoads and Fassihi, 2011; Austrade, 2008). Mobile service providers allow Iranians to use mobile phones, but the government controls and surveils this activity (Miller et al., 2023). The number of Internet users has continued to increase over time (Honari, 2015; World Bank, n.d.).

Iran's technology imports are another example of Iran facilitating ICTs. In 2022, Iran imported over \$3 billion in broadcasting equipment (9.5% of all imports) and over \$300 million in computers (1.3%). For the US, these rates were approximately 1.5% and 0.9%, respectively. For Türkiye, they were approximately 1.1% and 0.8% (OEC, n.d.-a; OEC, n.d.-b; OEC, n.d.-c (US, Iran, and Türkiye)). Iran's government has also encouraged domestic manufacturing and innovation in ICTs (Austrade, 2008), particularly within universities (Valori, 2023; Ashtarian, 2015). However, access to ICT hardware is heavily regulated by the government, as is the telecommunications industry and mobile phone market (Freedom House, 2018).

An example of blocking ICTs is Iran's filtering of Internet content. Since 2001, Iran has sought to control what information enters the country online, and has required ISPs to follow its filtering requirements. Iran has concentrated control of the Internet to the government, enabling widespread restriction of content across ISPs. Over time, filtering methods have improved, and Iran has passed laws redefining what content should be filtered and criminalizing online expression, including the "Cybercrimes Bill" of 2008. Iran also uses its control of the Internet to conduct extensive surveillance on web users ("Iran — OpenNet Initiative", n.d.).

Iran also uses this centralized Internet control to reduce Internet speeds and even shut down online or mobile services, especially during protests and elections. Overall, Iran's Internet speeds are low compared to its penetration rate, especially given that it has a robust ISP market (Honari, 2015; World Bank, n.d.). Iran disrupts and shuts down Internet service more frequently than every Asian country except China, and is currently blocking access to most major global social media platforms ("Internet shutdown tracker", n.d.). Iranian officials have at times planned to increase Internet speed and bandwidth (The Iran Project, 2016; Rezaian, 2023).

An early instance of control over Internet speed and availability was in 2006, when Iran's government required ISPs to reduce Internet speed, a move that was expected to hamper technological growth (Tait, 2018; "Iran — OpenNet Initiative", n.d.). During Iran's 2009 elections and subsequent protests, the government shut off mobile phone and SMS services and reduced speeds, and took similar actions in anticipation of the 2013 elections (Heacock and Faris, 2009; Shaheed, 2014). This pattern continued during protests in 2017-18 (Article 19, 2019; Center for Human Rights in Iran, 2018) and in 2022 (Axios, 2022; Polglase et al., 2022; Biddle and Hussein, 2022; Freedom House, 2018). Specifically, Iran's government has the ability to track device movements and communication data, redirect messages, put devices on slower networks, obtain extensive personal information from devices, and view Internet history, all in great detail. These strategies could be used to severely stall Internet usage and mobile communication for millions of Iranians (Biddle and Hussein, 2022; Miller et al., 2023). For a specific example, Iran's filtering system can "block a website within a few hours across the entire network in Iran" (Freedom House, 2018).

Overall, Iran's ICT policies forego social and economic benefits that alternative policies would generate, and have hampered technological innovation (Anderson, 2016). The government's ability to effectively turn off sections of the Internet, or at least restrict Internet use, risks interfering with banks and impeding "internet commerce," while local officials have admitted that slow Internet speeds disrupt everyday online business (Tajdin, 2013; Rezaian, 2023). Temporary blockages during protests and elections can cause substantial economic losses for business (Khosropour, 2018). Additionally, Iran's National Information Network risked interfering with foreign investment in Iran, and by creating a network detached from the global Internet, Iranian officials sacrificed access to the "expertise and resources" of existing technology (Rhoads and Fassihi, 2011). Finally, Iran has a relatively large young population that relies on the Internet and social media (Yee, 2022; Cincatta and Sadjadpour, 2017). Policies that block or slow down access to these platforms likely damage the state's public approval and could be partially responsible for low regime support in recent years (Hafezi, 2022; Aarabi et al., 2022).

Additionally, mobile operators in Iran have lost the equivalent of millions of dollars due to the country's policy of filtering Internet access (Salami, 2023). To bypass some of these restrictions, many Iranians purchase virtual private networks (VPNs), which can help them access websites that the National Information Network blocks, including social media (Dehghan, 2012; Castro, 2024). Sales of VPNs generate millions of dollars, but VPN providers are not taxed–so these sales do not economically benefit the Iranian government (Salami, 2023). Iran has taken steps to crack down on VPN use (Alterman, 2022).

Iran's filtering includes many of the most used international social media platforms. These include Facebook, X (formerly Twitter), Instagram, Youtube, Whatsapp, Telegram, and others. Some of these platforms have seen particular blockages during elections and protests, while many have been officially banned or restricted for years (Honari, 2015; Esfandiari, 2022; "Internet shutdown tracker", n.d.; Alterman, 2022; Sriram and Dubai newsroom, 2022). International media platforms like the New York Times and BBC are also blocked ("Iran — OpenNet Initiative", n.d.), in addition to streaming services

Iran's Third and Fourth Five-Year Development Plans (2000-2004 and 2005-2009) laid out steps to encourage ICT innovation, and in 2005 a government council started ICT infrastructure programs to help shift Iran toward a "knowledge economy" (UNCTAD, 2005; Amuzegar, 2010; Amiri and Sangar, 2023). The Fifth plan (2011-2016) encouraged science and technology innovation in universities (Ashtarian, 2015), and the Sixth plan (2017-2021) aimed to connect more households to the National Information Network (Bakhtiari, 2021). These efforts represent an effort by Iran's government to produce growth in the ICT sector (Amiri and Sangar, 2023), and they have been accompanied by government investments in ICTs (IRNA, 2016). Over the past few decades, Iran's ranking in the ICT Development Index has increased slightly, from 92 in 2002 to 81 in 2017 (IDI, 2009; IDI, 2017; IDI, 2023).

In 2006, Iran's Telecommunications Minister announced the development of the National Information Network, a domestic intranet controlled by the state (Center for Human Rights in Iran, 2014). It was intended to be deployed several years afterward, but delays pushed its official start to the late 2010s (Jafari, 2016). Its main purpose is enable online monitoring and censorship and to deter foreign access. Creating this network has been costly for Iran, whose ICT budget includes investment in the NIN. The NIN also contributes to Iran's ability to control international internet traffic, speed, and access (Millichronicle, 2020; Freedom House, 2018). When the government blocks or slows global networks during protests, the domestic National Information Network is left unaffected (Yee, 2022).

References

Aarabi, K., Shelley, J., & Blair, T. (2022). *Protests and Polling Insights From the Streets of Iran: How Removal of the Hijab Became a Symbol of Regime Change*. Retrieved March 15, 2024, from https://www.institute.global/insights/geopolitics-and-security/protests-and-polling-insights-streets-iran-how-removal-hijab-became-symbol-regime-change

Acemoglu, D., & Robinson, J. A. (2006). Economic Backwardness in Political Perspective [Edition: 2006/02/28 Publisher: Cambridge University Press]. *American Political Science Review*, *100*(1), 115–131. https://doi.org/10.1017/S0003055406062046

Akbarpour, N. (2022, December 6). *Gashaish, Sharif University class internet project*. BBC News Persian []. Retrieved February 2, 2024, from https://www.bbc.com/persian/articles/cekvyxjmnrjo
(Accessed in English using automatic Google Translate.)

Alterman, J. B. (2022). Protest, Social Media, and Censorship in Iran. *CSIS*. Retrieved February 5, 2024, from https://www.csis.org/analysis/protest-social-media-and-censorship-iran

Amiri, E., & Sangar, A. B. (2023). Assessing the ICT development in Iranian cities: The strategy to accelerate digital advancement. *Technological Forecasting and Social Change*, *197*, 122904. https://doi.org/10.1016/j.techfore.2023.122904

Amnesty International. (2020, November 16). *Iran: Internet deliberately shut down during November 2019 killings – new investigation*. https://www.amnesty.org/en/latest/press-release/2020/11/iran-internet-deliberately-shut-down-during-november-2019-killings-new-investigation/

Amuzegar, J. (2010). Iran's Fourth Plan: A Partial Assessment. *Middle East Policy*, *17*(4), 114–130. https://doi.org/10.1111/j.1475-4967.2010.00466.x

Anderson, C. (2016, September 23). *How Iran Is Building Its Censorship-Friendly Domestic Internet — WIRED*. Wired. https://www.wired.com/2016/09/how-iran-is-building-its-censorship-friendly-domestic-internet/

Arena, P., & Wolford, S. (2012). Arms, Intelligence, and War. *International Studies Quarterly*, *56*(2), 351–365. https://doi.org/10.1111/j.1468-2478.2012.00724.x

Arkin, W. M., Dilanian, K., & Windrem, R. (2019). *Pompeo says military action in Venezuela 'possible'*. CNN. https://www.cnn.com/2019/05/01/politics/mike-pompeo-venezuela-military-action/index.html

Article 19. (2019, October 14). *Tightening the net: Internet controls during and after Iran's protests*. Retrieved January 31, 2024, from https://web.archive.org/web/20191014103144/https://www.article19.org/resources/tightening-net-internet-controls-irans-protests/

Ashtarian, K. (2015). *15: Iran*. Retrieved March 10, 2024, from https://en.unesco.org/sites/default/files/usr15_iran.pdf

Associated Press. (2010). *Venezuelan national assembly bars foreign funding for NGOs*. The Guardian. https://www.theguardian.com/world/2010/dec/22/venezuela-chavez-ngo-foreign-funding

Austrade. (2008, July 27). *Information and communications technology (ICT) to Iran - For Australian exporters - Austrade*. Retrieved March 10, 2024, from https://web.archive.org/web/20080727015312/http://www.austrade.gov.au/ICT-to-Iran/default.aspx

Axios. (2022, September 21). *Internet restricted in Iran as anti-government protests intensify*. Axios. Retrieved March 10, 2024, from https://www.axios.com/2022/09/21/iran-protests-internet-restrictions-mahsa-amini

Badawy, A., Ferrara, E., & Lerman, K. (2018). Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 258–265. https://doi.org/10.1109/ASONAM.2018.8508646

Bakhtiari, F. (2021, February 1). *Iran among three countries with highest ICT growth: minister* [Section: Society]. Tehran Times. Retrieved March 10, 2024, from https://www.tehrantimes.com/news/457631/Iran-among-three-countries-with-highest-ICT-growth-minister

Bates, R. H. (1998). *Analytic Narratives*. Princeton University Press. https://books.google.com/books?id=BjV5HXIkw0gC

Baum, M. A. (2002). The Constituent Foundations of the Rally-Round-the-Flag Phenomenon. *International Studies Quarterly*, *46*(2), 263–298. https://doi.org/10.1111/1468-2478.00232

Baum, M. A. (2004). Going Private: Public Opinion, Presidential Rhetoric, and the Domestic Politics of Audience Costs in U.S. Foreign Policy Crises [Publisher: Sage Publications, Inc.]. *The Journal of Conflict Resolution*, *48*(5), 603–631. http://www.jstor.org/stable/4149812

BBC. (2009). Iran admits 4,000 June detentions. *BBC News*. http://news.bbc.co.uk/2/hi/middle_east/8195586.stm

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2012). Promoting transparency and accountability through ICTs, social media, and collaborative e-government. *Transforming Government: People, Process, and Policy*.

Biddle, S., & Hussein, M. (2022, October 28). *Hacked Documents: How Iran Can Track and Control Protesters' Phones*. The Intercept. Retrieved March 10, 2024, from https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/

Brooking, E. T., & Kianpour, S. (2020, February 12). *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*. Atlantic Council. Retrieved February 5, 2024, from https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/

Byrne, M. (2013). *CIA Confirms Role in 1953 Iran Coup*. The National Security Archives — The George Washington University. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB435/

Carson, A. (2016). Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War [Edition: 2015/10/05 Publisher: Cambridge University Press]. *International Organization*, *70*(1), 103–131. https://doi.org/10.1017/S0020818315000284

Carson, A. (2018). *Secret Wars: Covert Conflict in International Politics* (Vol. 157). Princeton University Press. https://doi.org/10.2307/j.ctv346p45

Castells, M. (2015). *Networks of outrage and hope: Social movements in the internet age*. Polity Press. https://books.google.com/books?id=MzDOCQAAQBAJ

Castro, C. (2024, February 23). *Iran outlaws "unauthorized" VPN usage*. TechRadar. Retrieved March 15, 2024, from https://www.techradar.com/computing/cyber-security/iran-outlaws-unauthorized-vpn-usage

Center for Human Rights in Iran. (2014, November 10). *The National Information Network (National Internet)* [Section: Internet freedom]. Retrieved January 31, 2024, from https://iranhumanrights.org/2014/11/internet-reportthe-national-information-network-national-internet/

Center for Human Rights in Iran. (2018, January 2). *Iran's Severely Disrupted Internet During Protests: "Websites Hardly Open"* [Section: Assembly / Association]. Retrieved March 6, 2024, from https://iranhumanrights.org/2018/01/irans-severely-disrupted-internet-during-protests-websites-hardly-open/

CFR Cyber Operations Tracker. (n.d.). *Cyber Operations Tracker*. Council on Foreign Relations. https://www.cfr.org/cyber-operations

CIA. (n.d.). *Iran*. CIA World Factbook. Retrieved March 8, 2024, from https://www.cia.gov/the-world-factbook/countries/iran/#economy

Cincatta, R., & Sadjadpour, K. (2017, December 18). *Iran in Transition: The Implications of the Islamic Republic's Changing Demographics*. Carnegie Endowment for International Peace. Retrieved March 13, 2024, from https://carnegieendowment.org/2017/12/18/iran-in-transition-implications-of-islamic-republic-s-changing-demographics-pub-75042

Clinton, H. (2011, October 14). *Secretary of State Clinton on Internet Freedom*. America.gov. Retrieved February 2, 2024, from https://web.archive.org/web/20111014002413/http://www.america.gov/st/texttrans-english/2010/January/20100121142618eaifas0.6585352.html

Cohen, Z. (2018). *North Korea accuses US of 'hatching a criminal plot to unleash a war'*. CNN. https://www.cnn.com/2018/08/27/politics/north-korea-us-special-forces-drill/index.html

Cormac, R., Walton, C., & Puyvelde, D. V. (2022). What constitutes successful covert action? Evaluating unacknowledged interventionism in foreign affairs [Edition: 2021/05/24 Publisher: Cambridge University Press]. *Review of International Studies*, *48*(1), 111–128. https://doi.org/10.1017/S0260210521000231

CSRC. (n.d.). *information and communications technology (ICT) - Glossary — CSRC*. NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/information_and_communications_technology

Debs, A., & Monteiro, N. P. (2013). Known Unknowns: Power Shifts, Uncertainty, and War. *International Organization*, *68*.

Dehghan, S. K. (2012). Iran set to block access to Google. *The Guardian*. Retrieved March 15, 2024, from https://www.theguardian.com/world/2012/sep/23/iran-block-access-google-gmail

Derakhshi, R. (2010). Iran accuses U.S. of seeking to use Internet against it. *Reuters*. Retrieved March 10, 2024, from https://www.reuters.com/article/idUSTRE60P426/

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, *21*(3), 69–83. https://www.journalofdemocracy.org/articles/liberation-technology/

Downes, A. B., & O'Rourke, L. A. (2016). You Can't Always Get What You Want: Why Foreign-Imposed Regime Change Seldom Improves Interstate Relations. *International Security*, *41*(2), 43–89. https://doi.org/10.1162/ISEC_a_00256

Doyle, K., & Kornbluh, P. (2017). *CIA and Assassinations: The Guatemala 1954 Documents* [National Security Archive Electronic Briefing Book No. 4: The George Washington University]. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB4/index.html

Dragu, T., & Lupu, Y. (2021). Digital Authoritarianism and the Future of Human Rights [Edition: 2021/02/09 Publisher: Cambridge University Press]. *International Organization*, *75*(4), 991–1017. https://doi.org/10.1017/S0020818320000624

Dubowitz, M. (2023, January 27). *Mapping the Protests in Iran*. FDD. https://www.fdd.org/analysis/2023/01/27/mapping-the-protests-in-iran-2/

Esfandiari, G. (2022, September 9). *Iran Accused Of Secretly Implementing Controversial Draft Internet Bill*. RadioFreeEurope/RadioLiberty. Retrieved March 6, 2024, from https://www.rferl.org/a/iran-internet-bill-controversy-secretly-implementing/32026313.html

Farrell, H. (2012). The Consequences of the Internet for Politics [Publisher: Annual Reviews]. *Annual Review of Political Science*, *15*(1), 35–52. https://doi.org/10.1146/annurev-polisci-030810-110815

Fathollah-Nejad, A. (2022, September 29). Can the Iranian System Survive? Retrieved February 5, 2024, from https://carnegieendowment.org/sada/88044

Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Oxford University Press. https://books.google.com/books?id=W3QjEAAAQBAJ

Feldstein, S. (2022). *DISENTANGLING THE DIGITAL BATTLEFIELD: HOW THE INTERNET HAS CHANGED WAR*. War on the Rocks. https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/

Fragile States Index. (2023). The Fund for Peace. https://fragilestatesindex.org/

Freedom House. (2018, November 1). *Freedom on the Net 2018 - Iran*. Refworld — UNHCR. Retrieved March 12, 2024, from https://www.refworld.org/reference/annualreport/freehou/2018/en/122294

Freedom House. (2023). *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*. Freedom House. https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence

Gainous, J., Wagner, K. M., & Abbott, J. P. (2015). Civic Disobedience: Does Internet Use Stimulate Political Unrest in East Asia? *Journal of Information Technology & Politics*, *12*(2), 219–236. https://doi.org/10.1080/19331681.2015.1034909

Gambrell, J. (2022, October 13). *Iran president accuses US of 'destabilization' amid protests*. AP News. Retrieved March 10, 2024, from https://apnews.com/article/iran-middle-east-dubai-united-arab-emirates-ali-khamenei-51fce3bad957ef64a6fc45a09301434e

Gerschenkron, A. (2014). Economic Backwardness in Historical Perspective. In *The globalization and development reader: Perspectives on development and global change*. Wiley.

Gershenkron, A. (1970). *Europe in the Russian Mirror: Four Lectures in Economic History*. Cambridge University Press. https://books.google.com/books?id=o32_KZakYpAC

GII. (2022). *IRAN (ISLAMIC REPUBLIC OF) — Global Innovation Index 2022*. World Intellectual Property Organization (WIPO). Retrieved March 10, 2024, from https://www.wipo.int/edocs/pubdocs/en/wipo_pub_2000_2022/ir.pdf

GII. (2023). *Iran (Islamic Republic of) ranking in the Global Innovation Index 2023*. World Intellectual Property Organization (WIPO). Retrieved March 15, 2024, from https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023/ir.pdf

Glanz, J., & Markoff, J. (2011). U.S. Underwrites Internet Detour Around Censors. *The New York Times*. Retrieved January 28, 2024, from https://www.nytimes.com/2011/06/12/world/12internet.html

Global Conflict Tracker. (2024, March 5). *Confrontation With Iran*. Council on Foreign Relations. Retrieved March 15, 2024, from https://cfr.org/global-conflict-tracker/conflict/confrontation-between-united-states-and-iran

Goemans, H., & Spaniel, W. (2016). Multimethod Research: A Case for Formal Theory. *Symposium on Qualitative and Multimethod Research*. https://doi.org/https://doi.org/10.1080/09636412.2016.1134176

Goodman, J., & Mustian, J. (2024). *AP investigation reveals secret U.S. spy program that targeted top Venezuelan officials*. PBS Newshour. https://www.pbs.org/newshour/politics/ap-investigation-reveals-secret-u-s-spy-program-that-targeted-top-venezuelan-officials

Gorgin, I. (2008). Looking Back At Tehran's 1999 Student Unrest. *Radio Free Europe/Radio Liberty*. Retrieved February 5, 2024, from https://www.rferl.org/a/Iran_Student_Protests/1182717.html

Graphika, S. I. O. (2022). Unheard Voice: Evaluating five years of pro-Western covert influence operations. *Stanford Digial Repository*. https://doi.org/https://doi.org/10.25740/nj914nx9540

Grzegorzewski, M., Spencer, M., & Brown, K. (2022, April 26). *In Search of Security: Understanding the Motives Behind Iran's Cyber-Enabled Influence Campaigns*. Modern War Institute. Retrieved February 5, 2024, from https://mwi.westpoint.edu/in-search-of-security-understanding-the-motives-behind-irans-cyber-enabled-influence-campaigns/

Hafezi, P. (2022). Insight: Many young Iranians lose their fear in struggle for "freedom". *Reuters*. Retrieved March 13, 2024, from https://www.reuters.com/world/middle-east/many-young-iranians-lose-their-fear-struggle-freedom-2022-11-03/

Hafezi, P. (2023). What has changed in Iran one year since Mahsa Amini protests erupted? *Reuters*. https://www.reuters.com/world/middle-east/what-has-changed-iran-one-year-since-mahsa-amini-protests-erupted-2023-09-11/

Haghighatnejad, R. (2016, February 17). *Iran's "Halal Internet" and the Battle for Online Freedom*. Iranwire.com. Retrieved February 2, 2024, from https://iranwire.com/en/society/61653/

Hansler, J., & De Vries, K. (2019). *Pompeo says military action in Venezuela 'possible'*. CNN. https://www.cnn.com/2019/05/01/politics/mike-pompeo-venezuela-military-action/index.html

Harmeet, K., Kim, A., & Sherman, I. (2020, January 11). *The US-Iran conflict: A timeline of how we got here*. CNN. Retrieved March 15, 2024, from https://www.cnn.com/interactive/2020/01/world/us-iran-conflict-timeline-trnd/

Heacock, R., & Faris, R. (2009, June 15). *Cracking Down on Digital Communication and Political Organizing in Iran — OpenNet Initiative*. OpenNet Iniative. Retrieved March 10, 2024, from https://opennet.net/blog/2009/06/cracking-down-digital-communication-and-political-organizing-iran

Honari, A. (2015). Online Social Research in Iran: A Need to Offer a Bigger Picture. *CyberOrient*, *9*(2), 6–32. https://doi.org/10.1002/j.cyo2.20150902.0002

Human Rights Watch. (1999, July 30). *New Arrests And "Disappearances" Of Iranian Students (Press Release, July 1999)*. Human Rights Watch. https://www.hrw.org/legacy/press/1999/jul/iran730.htm

Hussein, F. (2022, September 23). *US allows tech firms to boost internet access in Iran*. AP News. Retrieved March 10, 2024, from https://apnews.com/article/iran-technology-middle-east-internet-access-5037431302763edc8fa2cf72c4c44011

IDI. (2009). *Measuring the information society – the ICT development index*. International Telecommunication Union. Retrieved March 12, 2024, from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2009.aspx

IDI. (2017). *Measuring the Information Society Report 2017*. International Telecommunication Union. Retrieved March 12, 2024, from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

IDI. (2023). *Measuring digital development — the ICT development index 2023*. International Telecommunication Union Development Sector. Retrieved March 15, 2024, from https://www.itu.int/itu-d/reports/statistics/idi2023/

Internet shutdown tracker. (n.d.). Surfshark. Retrieved January 31, 2024, from https://surfshark.com/research/internet-censorship

Iran — OpenNet Initiative. (n.d.). OpenNet Iniative. https://opennet.net/research/profiles/iran

Iran International. (2023a, July 24). *Iran Accuses US Of Destabilizing Acts In Cybersphere*. Retrieved March 10, 2024, from https://www.iranintl.com/en/202307243236

Iran International. (2023b, September 24). *Iran Approves Full Internet Access SIM Cards For Foreign Tourists*. Retrieved February 2, 2024, from https://www.iranintl.com/en/202309248402

IRNA. (2016, September 6). *Iran to invest $18bln in Information, Communications Technology, says minister*. Zawya. Retrieved March 12, 2024, from https://www.zawya.com/en/business/iran-to-invest-18bln-in-information-communications-technology-says-minister-w8yy6cia

Isfahani, S. (2022, July 25). *The Internet has no place in Khamenei's vision for Iran's future*. Atlantic Council. Retrieved March 10, 2024, from https://www.atlanticcouncil.org/blogs/iransource/the-internet-has-no-place-in-khameneis-vision-for-irans-future/

Jafari, H. (2016, August 29). *Iran Initiates the First Phase of the National Information Network* [Section: Featured]. TechRasa. Retrieved March 6, 2024, from https://techrasa.com/2016/08/29/iran-initiates-first-phase-national-information-network/

Johnson, L. (2021). *The Third Option: Covert Action and American Foreign Policy*. Oxford University Press. https://books.google.com/books?id=QbNLEAAAQBAJ

Joseph, M. F., & Poznansky, M. (2018). Media technology, covert action, and the politics of exposure [Publisher: Sage Publications, Inc.]. *Journal of Peace Research*, *55*(3), 320–335. https://www.jstor.org/stable/48595886

Kamarck, E., & Muchnick, J. (2023, February 23). *One year into the Ukraine war — What does the public think about American involvement in the world?* Brookings. https://www.brookings.edu/articles/one-year-into-the-ukraine-war-what-does-the-public-think-about-american-involvement-in-the-world/

Kapusta, P. (2015). The Gray Zone. *Special Warfare*. https://www.proquest.com/docview/1750033789?sourcetype=Trade%20Journals

Kaviani, H. (2022). U.S. Encourages Technology Companies To Help Iranians Circumvent Internet Outages. *Radio Free Europe/Radio Liberty*. Retrieved March 10, 2024, from https://www.rferl.org/a/us-encourages-technology-companies-to-help-iranians-circumvent-internet-outages/32080550.html

Kenyon, P. (2013, February 4). *Iran's Leader Embraces Facebook; Fellow Iranians Are Blocked*. NPR. Retrieved March 15, 2024, from https://www.npr.org/2013/02/04/171064466/irans-leader-embraces-facebook-fellow-iranians-are-blocked

Khosropour, A. (2018). Iran without internet; What sectors suffer the most? *BBC News [Persian]*. Retrieved March 6, 2024, from https://www.bbc.com/persian/iran-features-50489064 (Accessed in English using automatic Google Translate.)

Kiley, J., & Dougherty, C. (2023, March 14). *A Look Back at How Fear and False Beliefs Bolstered U.S. Public Support for War in Iraq*. https://www.pewresearch.org/politics/2023/03/14/a-look-back-at-how-fear-and-false-beliefs-bolstered-u-s-public-support-for-war-in-iraq/

King, R. R. (2019). North Koreans Want External Information, But Kim Jong-Un Seeks to Limit Access. *Center for Strategic and International Studies*. https://www.csis.org/analysis/north-koreans-want-external-information-kim-jong-un-seeks-limit-access

Lake, E. (2016). Why Obama Let Iran's Green Revolution Fail. *Bloomberg.com*. https://www.bloomberg.com/view/articles/2016-08-24/why-obama-let-iran-s-green-revolution-fail

Lansberg-Rodriguez, D. (2015). Coup Fatigue in Caracas. *Foreign Policy*. https://foreignpolicy.com/2015/03/15/coup-fatigue-in-caracas-venezuela-maduro/

Leonida, L., Patti, D. M. A., & Navarra, P. (2013). Testing the Political Replacement Effect: A Panel Data Analysis*. *Oxford Bulletin of Economics and Statistics*, *75*(6), 785–805. https://doi.org/10.1111/j.1468-0084.2012.00716.x

Levin, D. H. (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results. *International Studies Quarterly*, *60*(2), 189–202. https://doi.org/10.1093/isq/sqv016

Loft, P. (2023). 2022 Iran protests: Human rights and international response. *House of Commons Library*. https://commonslibrary.parliament.uk/research-briefings/cbp-9679/

Lowenthal, M. M. (2023). *Intelligence: From Secrets to Policy* (9th ed.). CQ Press.

Lum, T., & Figliola, P. M. (2012). China, Internet Freedom, and U.S. Policy. *Congressional Research Service*. Retrieved February 14, 2024, from https://sgp.fas.org/crs/row/R42601.pdf

MacLellan, S. (2018, January 9). *What You Need to Know about Internet Censorship in Iran*. Centre for International Governance Innovation. Retrieved January 24, 2024, from https://www.cigionline.org/articles/what-you-need-know-about-internet-censorship-iran/

Maheshwari, S., & Holpuch, A. (2024). Why the u.s. is weighing whether to ban tiktok. *The New York Times*. https://www.nytimes.com/article/tiktok-ban.html

Majidyar, A. (2018, April 26). *Iran revokes Telegram license as authorities step up Internet crackdown*. Middle East Institute. Retrieved March 15, 2024, from https://www.mei.edu/publications/iran-revokes-telegram-license-authorities-step-internet-crackdown

Maloney, S. (2013). *Remembering Iran's Student Protests, Fourteen Years Later*. Brookings. https://www.brookings.edu/articles/remembering-irans-student-protests-fourteen-years-later/

Milani, A. (2010, October 6). *The Green Movement — The Iran Primer*. United States Institute of Peace. Retrieved February 5, 2024, from https://iranprimer.usip.org/resource/green-movement

Miller, G., Al-Jizawi, N., Ermoshina, K., Michaelsen, M., Panday, Z., Plumptre, G., Senft, A., & Deibert, R. (2023, January 16). *You Move, They Follow: Uncovering Iran's Mobile Legal Intercept System* (Section: Transparency and Accountability). Citizen Lab, University of Toronto. Retrieved March 10, 2024, from https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/

Millichronicle. (2020, November 1). *Iran's Intranet: a Master Plan for Internet Censorship*. Millichronicle. Retrieved March 16, 2024, from https://millichronicle.com/2020/11/irans-intranet-a-master-plan-for-internet-censorship.html

Mueller, J. E. (1970). Presidential Popularity from Truman to Johnson [Edition: 2014/08/01 Publisher: Cambridge University Press]. *American Political Science Review*, *64*(1), 18–34. https://doi.org/10.2307/1955610

Myrick, R. (2021). Do External Threats Unite or Divide? Security Crises, Rivalries, and Polarization in American Foreign Policy [Edition: 2021/04/20 Publisher: Cambridge University Press]. *International Organization*, *75*(4), 921–958. https://doi.org/10.1017/S0020818321000175

OEC. (n.d.-a). *Iran (IRN) Exports, Imports, and Trade Partners*. The Observatory of Economic Complexity. Retrieved March 12, 2024, from https://oec.world/en

OEC. (n.d.-b). *Turkey (TUR) Exports, Imports, and Trade Partners*. The Observatory of Economic Complexity. Retrieved March 12, 2024, from https://oec.world/en

OEC. (n.d.-c). *United States (USA) Exports, Imports, and Trade Partners*. The Observatory of Economic Complexity. Retrieved March 12, 2024, from https://oec.world/en

OECD. (n.d.-a). *Information and communication technology (ICT)*. OECD iLibrary. https://www.oecd-ilibrary.org/science-and-technology/information-and-communication-technology-ict/indicator-group/english_04df17c2-en

OECD. (n.d.-b). *Internet and communication technology (ict) - internet access*. OECD Data. https://data.oecd.org/ict/internet-access.htm

Osborne, M. (2004). *An Introduction to Game Theory*. Oxford University Press. https://books.google.com/books?id=V2zAkgEACAAJ

Pietsch, B. (2024). How the U.S. and Iran escaped a broader conflict in 2020. *Washington Post*. Retrieved March 15, 2024, from https://www.washingtonpost.com/world/2024/02/01/us-iran-conflict-biden-trump/

Pleming, S. (2009). U.S. State Department speaks to Twitter over Iran. *Reuters*. Retrieved January 28, 2024, from https://www.reuters.com/article/idUSWBT011374/

Polglase, K., Mezzofiore, G., & Kent, L. (2022, October 4). *The US says it's helping Iranians navigate a massive internet blackout. Activists say it's too little, too late*. CNN. Retrieved March 10, 2024, from https://www.cnn.com/2022/10/04/world/iran-internet-blackout-intl-cmd/index.html

Psaledakis, D., Lewis, S., & Psaledakis, D. (2022). U.S. adjusts sanctions to help Iranians evade online surveillance, censorship. *Reuters*. Retrieved March 10, 2024, from https://www.reuters.com/world/us-expands-sanctions-exceptions-help-provide-internet-iranians-2022-09-23/

Ranalli, R. (2022). *Civil upheaval in Iran: Why widespread discontent with the country's religious regime may have reached a tipping point*. Harvard Kennedy School. https://www.hks.harvard.edu/faculty-research/policy-topics/international-relations-security/civil-upheaval-iran-why-widespread

Rezaian, J. (2023). Internet improvements in store for Iran. *Washington Post*. Retrieved January 28, 2024, from https://www.washingtonpost.com/world/middle_east/internet-improvements-in-store-for-iran/2014/02/13/b3d730fe-8ea4-11e3-878e-d76656564a01_story.html

Rhoads, C., & Fassihi, F. (2011). In Censorship Move, Iran Plans Its Own, Private Internet. *Wall Street Journal*. Retrieved February 2, 2024, from http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html

Salami, M. (2023, August 22). *Internet Filtering in Iran Boosts VPN Business - Much of it Government-Owned • Stimson Center*. Stimson Center. Retrieved January 31, 2024, from https://www.stimson.org/2023/internet-filtering-in-iran-boosts-vpn-business-much-of-it-government-owned/

Sanger, D. E. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Seifi, E. (2023, May 23). *But and ifs of 'Class Internet*. Islamic Republic News Agency. Retrieved February 2, 2024, from https://www.irna.ir/news/85109750/%D8%A7%D9%85%D8%A7-%D9%88-%D8%A7%DA%AF%D8%B1%D9%87%D8%A7%DB%8C-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%B7%D8%A8%D9%82%D8%A7%D8%AA%DB%8C
(Accessed in English using automatic Google Translate.)

Shaheed, A. (2014, July 5). *Ahmed Shaheed ≫ Layers of Internet Censorship in Iran*. UN Special Rapporteur on the Situation of Human Rights in the Islamic Republic of Iran. Retrieved March 10, 2024, from https://www.shaheedoniran.org/english/blog/layers-of-internet-censorship-in-iran/

Shalal-Esa, A. (2013). Iran strengthened cyber capabilities after Stuxnet: U.S. general. *Reuters*. Retrieved February 5, 2024, from https://www.reuters.com/article/idUSBRE90G1C4/

Sharifi, K. (2024). Growing 'Despondency' And Hard-Liners' Dominance: Key Takeaways From Iran's Elections. *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/iran-elections-key-takeaways-khamenei-raisi/32850541.html

Shirky, C. (2008). *Here Comes Everybody: The Power of Organizing Without Organizations*. Penguin Press.

Shortridge, A. (2021, October 1). *The U.S. War in Afghanistan Twenty Years On: Public Opinion Then and Now*. Council on Foreign Relations. https://www.cfr.org/blog/us-war-afghanistan-twenty-years-public-opinion-then-and-now

Smeltz, D., Daalder, I. H., Friedhoff, K., Kafura, C., & Sullivan, E. (2022). *2022 Survey of Public Opinion on US Foreign Policy* (Research). The Chicago Council on Global Affairs. Retrieved March 15, 2024, from https://globalaffairs.org/research/public-opinion-survey/2022-chicago-council-survey

Sohrabi-Haghighat, H. M., & Mansouri, S. (2010). 'WHERE IS MY VOTE?' ICT Politics in the Aftermath of Iran's Presidential Election. *International Journal of Emerging Technologies and Society*, *8*(1), 24–41. Retrieved January 28, 2024, from https://dev.sssup.it/UploadDocs/13478_8_R_ICT__Politics__in__the__Aftermath__of__Iran__Presidential__Election_13.pdf

Sriram, A., & Dubai newsroom. (2022). As unrest grows, Iran restricts access to Instagram, WhatsApp. *Reuters*. Retrieved March 12, 2024, from https://www.reuters.com/world/middle-east/iran-restricts-access-instagram-netblocks-2022-09-21/

Stein, E. A. (2017). Are ICTs Democratizing Dictatorships? New Media and Mass Mobilization*. *Social Science Quarterly*. https://doi.org/https://doi.org/10.1111/ssqu.12439

Stelzenmüller, C. (2017, June 28). The Impact of Russian Interference on Germany's 2017 Elections [Testimony before the U.S. Senate Select Committee on Intelligence]. Retrieved November 11, 2023, from https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf

Stout, M. (2017). Covert Action in the Age of Social Media. *Georgetown Journal of International Affairs*, *18*(2), 94–103. https://www.jstor.org/stable/26396023

Tait, R. (2018, September 26). *Iran bans fast internet to cut west's influence — World news — The Guardian*. The Guardian. Retrieved March 10, 2024, from https://web.archive.org/web/20180926025132/https://www.theguardian.com/technology/2006/oct/18/news.iran

Tajdin, B. (2013). Will Iran's national internet mean no world wide web? *BBC News*. Retrieved January 23, 2024, from https://www.bbc.com/news/world-middle-east-22281336

The Iran Project. (2016, April 17). *Minister: Iran Internet bandwidth to increase to 12,000 Gbits*. The Iran Project. Retrieved March 12, 2024, from https://www.theiranproject.com/en/news/209900/minister-iran-internet-b_andwidth-to-increase-12-000-gbit-s

Thrall, A. T. (2017, February 16). *77. Public Opinion on U.S. Foreign Policy*. Cato Institute. https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/77-public-opinion-us-foreign-policy

Toor, A. (2013, December 4). *If an ayatollah tweets in Iran, who hears it?* The Verge. Retrieved February 2, 2024, from https://www.theverge.com/2013/12/4/5174282/ayatollah-rouhani-tweet-in-iran-but-social-media-ban-remains

Torbati, Y. (2012). Internet ayatollah: Iran's supreme leader "likes" Facebook. *Reuters*. Retrieved February 2, 2024, from https://www.reuters.com/article/idUSBRE8BG0S1/

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From Liberation to Turmoil: Social Media and Democracy. *Journal of Democracy*, *28*(4), 46–59. https://www.journalofdemocracy.org/articles/from-liberation-to-turmoil-social-media-and-democracy/

U.s. relations with the democratic people's republic of korea. (2021). United States Department of State. https://www.state.gov/u-s-relations-with-north-korea/

U.S. Relations With Venezuela. (2023). United States Department of State. https://www.state.gov/u-s-relations-with-venezuela/

UNCTAD. (2005). *Science, Technology and Innovation Policy Review — The Islamic Republic of Iran*. Retrieved March 10, 2024, from https://unctad.org/system/files/official-document/iteipc20057_en.pdf

Valdivia, A. N. (1991). The U.S. Intervention in Nicaraguan and Other Latin American Media. In *Revolution and counterrevolution in nicaragua* (1st ed.). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429304682-16/intervention-nicaraguan-latin-american-media-angharad-valdivia

Valori, G. E. (2023, July 5). *Iran, technology and innovation*. Modern Diplomacy. Retrieved March 10, 2024, from https://moderndiplomacy.eu/2023/07/05/iran-technology-and-innovation/

Warren, T. C. (2014). Not by the Sword Alone: Soft Power, Mass Media, and the Production of State Sovereignty [Publisher: [The MIT Press, University of Wisconsin Press, Cambridge University Press, International Organization Foundation]]. *International Organization*, *68*(1), 111–141. http://www.jstor.org/stable/43282097

Wilde, G., & Sherman, J. (2022, March 14). *Targeting Ukraine through Washington: Russian election interference, Ukraine, and the 2024 US election*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington/

World Bank. (n.d.). *Individuals using the Internet (% of population) — International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database*. World Bank Open Data. Retrieved January 31, 2024, from https://data.worldbank.org

Yang, M. (2013). The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response. *Northwestern Journal of Technology and Intellectual Property*, *11*(7). Retrieved March 15, 2024, from https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/7/

Yee, V. (2022). Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage. *The New York Times*. Retrieved March 12, 2024, from https://www.nytimes.com/2022/09/29/world/middleeast/iran-internet-censorship.html

Young, M. K. (2020, March 5). *New Evidence Shows How Russia's Election Interference Has Gotten More Brazen — Brennan Center for Justice*. Brennan Center for Justice. Retrieved March 13, 2024, from https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more