



Munich Personal RePEc Archive

On Principal Agents, Rogue Agencies and Systemic Government Failure: A Case Study

Otterson, James

International Monetary Fund

20 June 2023

Online at <https://mpra.ub.uni-muenchen.de/118023/>
MPRA Paper No. 118023, posted 27 Jul 2023 06:36 UTC

On Principal Agents, Rogue Agencies and Systemic Government Failure: A Case Study

James Otterson

*International Monetary Fund (IMF)*¹

This note sums up a US Congress Committee Investigation Report (CIR) on abuses carried out by intelligence agents of the Department of Commerce (DOC) over the last twenty years. We also consider some possible background contexts underlining the issues covered by the CIR along with preventive policy considerations.

In terms of economic theory, this is an account of how principal agents built a rogue government agency that potentially triggered a systemic failure of part of the US government. We consider the mechanisms that enabled the underlining principal agent problems and mitigating factors for each given mechanism.

JEL code: H830

Introduction

In 2021, the US Congress carried a Congressional Investigation² on how the Investigations and Threat Management Services (ITMS), a small division of the DOC assigned to oversee the security and safety of the department's buildings and directors, evolved into an intelligence agency with police powers. This evolution took place outside the established government operational procedures. Without proper oversight and with ample powers, the ITMS scoured the lives of DOC workers, members of Congress, and US citizens. Its acts were not restricted to spying on individuals but they also included the sabotage of lives and careers of people the division knew to be innocent. For over a decade, more than 24 ITMS agents, many of which suffered retaliations for their actions, reported the division's abusive behavior to a variety of oversight agencies. Despite their efforts, it is likely that effective actions against the division, including the CIR on it, were taken only after a Washington Post article³ was published on it in 2021. The issues raised by the CIR are still of concern since it is unclear if the ITMS mode of operation has spread to other parts of government.

This note is structured as follows. It begins with a short description of the relevant government agencies. After that, it describes the path the ITMS took to become an intelligence agency with police powers and how it organized itself and trained its agents to perform its new functions. The note then covers specific cases of how the ITMS exerted its powers. Finally, this note considers possible broader contexts that enabled the ITMS actions and, for each case, potential preventive measures to ensure that the ITMS misconduct is not repeated at other parts

¹ The views expressed in this paper are from the author and do not necessarily represent the views of the IMF, its Executive Board, or IMF management. Much of this work was completed while the author was working at the Congressional Budget Office (CBO). The views expressed here should not be interpreted as CBO's. The author is grateful to the valuable comments of the many colleagues that served to broaden the scope of the analysis.

² US Congress. *Committee Investigation Report - Abuse and Misconduct at the Commerce Department*. July 2021

³ Shawn Boburg. *Commerce Department security unit evolved into counterintelligence-like operation*. Washington Post, May 2021

of government. A conclusion section ends the note.

Institutional Context

The issues addressed by the CIR mainly cover the actions of three government agencies: the ITMS of the DOC, the US Marshals Services (USMS) of the Justice Department, and the Office of the Director of National Intelligence (ODNI).

THE DOC was founded in 1903 in order to promote the US economic development. It currently has a large portfolio, including carrying out the census, the production of the most essential macroeconomic and industrial production indicators, the concession of patents, the promotion of measurement standards, and the collection of information on climate and oceanic conditions. It has approximately 45 thousand employees and it runs on the lowest budget of the current 15 government departments (\$8 billion dollars in 2021). The ITMS is a small division of the DOC's Security Department. It was created in 2000 with the mandate to protect the DOC's buildings and its director.

THE USMS is a federal policy force of the Justice Department serving the Judiciary branch. It has around 4,000 employees and it is responsible for safeguarding the Judiciary buildings and employees, and arresting criminals at large, among other police force activities. Created in 1789, it is the oldest US law enforcement agency.

THE US INTELLIGENCE COMMUNITY (IC) includes the operation of 16 government agencies spread over 6 departments of government, besides one agency that is not under any department (the CIA). Since the passage of the Intelligence Reform and Terrorism Prevention Act⁴, the IC agencies are supervised by the ODNI, a function formerly attributed to the CIA, whose director was by default the Director of National Intelligence (DNI). The IC's budget and number of workers are not made public. However, the number of people with a security clearance that grants access to national security information is about 850,000 people⁵.

⁴ US Congress. *Intelligence Reform and Terrorism Prevention Act*. December 2004

⁵ Dana Priest and William Arkin. *A hidden world, growing beyond control*. Washington Post, June 2010. URL <https://www.washingtonpost.com/topsecretamerica>

How the ITMS became an intelligence agency with police powers

Initially, the ITMS scope was restricted to protection services. It had a specific mandate to protect the DOC's director and the department's buildings. The ITMS did not have police enforcement powers or the right to carry out activities related to national security issues.

TO GET POLICE ENFORCEMENT POWERS, the ITMS resorted to the USMS. Under specific circumstances, USMS agents can deputize people outside their agency, granting them police powers. ITMS members were deputized by the USMS with a mandate to protect the DOC's "critical infrastructure"⁶. The vague definition of the this term, coupled with the ample array of activities carried out by the DOC, granted the ITMS a wide range of action. After being deputized, ITMS agents started to conduct criminal investigations, make arrests, and carry weapons in public spaces (including on flights).

⁶ See the CIR pages 4, 6, 10 and 17. The CIR's page 14 lists several problems with the USMS deputation program. It is worth noticing that even the USMS ended up denouncing the actions of the ITMS agents to the Office of the Inspectors General (OIG) stating that they were biased against minorities (see the CIR page 35).

TO GET INTELLIGENCE AGENCY POWERS, the ITMS initially used the services of the Office of the Executive Support (OES) to get access to the IC, the standard way a federal agency outside the IC can request its services. However, over time the ITMS started viewing the OES as road block to an interaction with IC agencies and acted to get direct access to them. To that end, the ITMS used its police powers to launch a security violation investigation on all OES employees. The process included a mass interrogation of OES employees and, in the end, three OES employees were referred to the DOJ for potential lawsuits; all cases were later dropped⁷. After this investigation, the ITMS got a direct line of access to the IC under minimal supervision and started to act as if it had the authority to conduct counter-intelligence activities⁸. Indeed, a formal complaint of a special agent states that the ITMS operated as a FBI, CIA, and NSA agencies rolled up together with minimal supervision⁹. Seeking some legitimacy, the ITMS reported its actions directly to the ODNI, the office created to supervise the whole IC. An ODNI assessment of the ITMS activities concluded that it was important for the ITMS to be involved with counter-intelligence operations, that the ITMS initiatives were excellent and that they had the potential to be extended to other parts of the government¹⁰.

⁷ See the CIR page 15 for the initial interaction between the ITMS and the OES. See page 32 for how the ITMS acted against the OES to get direct access to the IC.

⁸ See the CIR pages 4, 14 to 19, 30, 31 and 34.

⁹ CIR page 17

¹⁰ See CIR page 16.

Despite having only a tenuous mandate to carry out police or intelligence agency work, over the year the ITMS cemented its activities in these directions. By 2017, the DOC budget submitted to congress was describing the ITMS as a division that fulfilled the national strategic needs on counterintelligence, transnational crime and counter-terrorism by investigating grave national security threats¹¹.

¹¹ The DOC 2011 budget already had a similar description the ITMS function (CIR page 15).

How the ITMS trained its agents

THE MANNER IN WHICH THE ITMS TRAINED ITS AGENTS IS INDICATIVE OF HOW IT OPERATED IN GENERAL. Overall, the CIR concludes that the ITMS managers were not qualified to run a police force unit or an intelligence agency and that the training they gave to their em-

¹² CIR page 25.

ployees was focused on how to carry out clandestine operations¹².

More specifically, several agents stated to the CIR that the training they got while working at the ITMS diverged from the expected federal government standards and included: chasing the ITMS director's car in high speeds; being confronted by actors while armed in banks or federal government building, without knowing that it was a training exercise; and taking forensic analysis courses given by the ITMS director, a person without qualifications in the field. The ITMS director himself did not complete the basic training required for criminal investigators, and he also failed to obtain the required USMS qualification for deputized agents.

¹³ CIR page 22.

THE ITMS MODE OF OPERATION reflected its disregard towards basic training. There were no established internal guidelines in place. For instance¹³, although the division carried out police investigations, it did not document them. It also did not follow the guidelines on how to handle collected evidence materials. Furthermore, untrained ITMS agents interviewed and interrogated people without informing them of their basic constitutional rights. The agency ended up opening a large number of weak cases that were never closed.

Specific Cases

ACTING AS A POLICE FORCE AND A NATIONAL SECURITY AGENCY, and without much oversight, the ITMS disrupted the lives of innocent people sabotaged careers, invaded the privacy of members of the public, and retaliated against the agents that tried to correct its mode of operation. The ITMS actions demonstrate the destructive power a small number of badly-trained public servants have when they have access to modern surveillance tools and employ abusive police tactics.

OF THE CASES REFERRED TO PROSECUTION by the ITMS, perhaps the most salient ones are that of Sherry Chen and Chunzai Wang¹⁴.

¹⁴ See the CIR pages 12 and 13 for these cases. The ITMS referred many cases for prosecution but the DOJ regularly declined to bring them forward (CIR page 4).

SHERRY CHEN is a award winning hydrologist at the DOC's National Oceanic and Atmospheric Administration (NOOA). She was investigated and interrogated by the ITMS on the suspicion that she was a Chinese spy. A case against her was brought to court based on a public domain material she forwarded to a foreign national. In 2014 she was placed under arrest while waiting for her trial but all charges against her were dropped at the beginning of it. The defendant points to potentially gross misconduct on the part of the ITMS including being pressured by ITMS agents to sign a document stating she was guilty,

and had been advised by them to not seek legal counsel. Chen continues to be on the DOC's payroll but she has been placed on administrative leave since the end of her trial. In 2022 Chen reached a settlement with the DOC over a malicious prosecution and false arrest lawsuit¹⁵.

¹⁵ Kimmy Yam. *After being falsely accused of spying for China, Sherry Chen wins significant settlement.* NBC News, November 2022

CHUNZAI WANG is a top scientist working on the impact of climate change on the ocean working at the NOAA. His participation on a Chinese talent development program triggered and ITMS investigation. Wang was interrogated by the ITMS, his house was searched for evidence, and he spend a day in jail while waiting for his trial. Initially, the prosecutors sought 5-year jail sentence but later all criminal charges against him were dropped.

THE ITMS ACTS OF SABOTAGE against DOC workers apparently started after it became clear it could hardly win the judicial cases it wanted to bring against them. Employing clandestine operation tactics, the ITMS regularly searched the office space of DOC workers it considered suspect¹⁶. These investigations were done by agents wearing a balaclava and shoe nets, after they had turned off the internal circuit cameras in order to leave no trace and keep the investigation off the record. The agents searched employees' computers, email accounts, and cell phone data. The CIR states that the ITMS scoured the lives of many DOC employees, including accessing their information on intelligence agency databases (which presumably carry detailed real-time information), just because their names differed from standard white American ones¹⁷. A whistle-blower states that xenophobia was the main motivator of the ITMS actions and that the ITMS actions were focused on ethnic minorities, foreign visitors, and people with connections to these types of people. The CIR also states that once a case was opened against a DOC employee it was unlikely to ever be closed, and that many were classified as "related to terrorist acts".

¹⁶ See the CIR page 12. On the same page, the CIR concludes that many of the ITMS investigations on DOC employees were based on limited evidence.

¹⁷ CIR pages 18 and 19.

The extreme surveillance employed by the ITMS on DOC employees were used to inform its acts of sabotage. In one case¹⁸, a worker from a ethnic minority group was investigated by the ITMS for over 4 years without a clear case against her. No supporting evidence of criminal activities was found even though she was put under surveillance at work and in her house. An ITMS agent quoted by the CIR stated that the aim was to make the employee isolated at work and to force her to quit her job under enormous pressure.

¹⁸ CIR page 18.

THE ITMS INVESTIGATED MANY US CITIZENS AND MEMBERS OF CONGRESS. At least one member of congress was investigated by the ITMS after he sent a letter to the DOC director with some questions on the US census process. The ITMS used mass-surveillance tools to

¹⁹ CIR page 19.

track comments made in social media platforms about the DOC¹⁹. A case covered by the CIR details how an elderly man with few followers on Facebook was investigated by the ITMS after he criticized the US census on that platform. This case, among similar ones, were then sent to the FBI for further investigation. The FBI would invariably drop these criminal investigations claiming that the people being investigated were only exercising their freedom of speech rights with conversations that did not pose a threat to national security. The ITMS, however, never closed any of these cases. Another case covered by the CIR started when a group of middle school students sent a letter to the DOC asking for a whale species to be included into the list of endangered species. This prompted the ITMS to open a case on these students and a detailed investigation on the letter's main author, a middle school student herself²⁰.

²⁰ CIR page 33.

²¹ CIR page 27, for example.

THE ITMS ROUTINELY RETALIATED AGAINST AGENTS that raised internal or external complaints about the division's mode of operation. The CIR covers several cases where the ITMS sought to lower the security clearance of these agents²¹. Such an action can derail or end the career of a security agent. The ITMS did not shy away from retaliating against any agent that got in its way, not even decorated soldiers or agents from other agencies. The courage displayed by these agents is notable. Even though they were probably well aware of the retaliation they would face from the ITMS, which could end their careers or send them to jail, they still denounced the ITMS to several government agencies. Their accounts seem to form the core of the CIR.

Broader context

Below, we consider some possible reasons for the institutional failure that allowed the ITMS to operate in an abusive manner: tail event, the dismantling of the federal government, the new government operational procedures triggered by the 9/11 terrorist attacks, and the US transition into a security state. Different reasons lead to different ways to prevent the abusive behavior similar to the one done by the ITMS.

²² CIR page 21.

IT COULD BE THAT THE IDIOSYNCRATIC AND TEMPORARY mismanagement of several US government agencies is what failed to prevent the ITMS' abusive behavior, that is, it was a tail event, namely a random, albeit very unlikely, event. The CIR concludes that the ITMS was chronically mismanaged and that it had a culture of rampant disregard towards government norms²². For its extreme abusive behavior to be able to happen, however, the ITMS mismanagement had to be aligned with failures in other parts of government, such as:

- the USMS deputation program²³;
- the DOC upper management that was informed on the actions of the ITMS, investigated them and concluded that the division did not have the authority to employ broad police powers²⁴ but did not act to prevent them²⁵;
- the OIG, whose mandate is to investigate abuses and misconducts of government agencies before they become the subject of a congressional investigation but after investigating the ITMS it did nothing to prevent the division's violations of civil liberties and constitutional rights²⁶;
- the DOJ that received many trial cases from the ITMS based on weak evidence, some of which were dropped during trial, but these did not raise red flags in the department;
- the ODNI that allowed and encouraged a small division outside the IC to act as an intelligence agency under minimal supervision.

If the random alignment of failures of US government agencies is what allowed the ITMS actions to take hold then preventing similar misconduct would involve reducing the probability and duration of such events. Reinforcing the role of agencies such as the OES that provide formal ways for government divisions to interact should decrease the chance of mismanaged divisions to collaborate. Strengthening the role of the OIG should not only provide a deterrent to agency misconduct but, since it has a mandate to investigate and redress issues, it can also provide a quick process to end the abusive behavior of an agency.

THE DISMANTLING OF GOVERNMENT INSTITUTIONS could be a more systemic explanation that led to the failure of several government agencies in preventing the ITMS misconduct. It is worth noting in this direction that the position meant to oversee the ITMS remained vacant over many years²⁷. In the opposite direction, one can argue that the problem is not the dismantling of the government institutions but its rapid expansion. In the ITMS case, several agents related to the CIR that the ITMS main goal was to expand its powers as fast as possible²⁸. One could argue in these lines that the problem here was a dismantling of government institutions alongside the quick expansion of the ones covering national security issues²⁹. This would explain the rapid transformation, under minimal supervision, of the ITMS into an intelligence agency with police powers. If this line of thought is correct, to prevent institutional behavior similar to the ITMS' misconducts, guidelines should be put in place for rapid expanding (security related) agencies, and the dismantling of government institutions

²³ CIR page 14.

²⁴ CIR pages 20 and 21.

²⁵ Maybe even the DOC upper management was powerless against the ITMS. One of the secretary of commerce built a Faraday cage in his office to prevent being eavesdropped. See also the CIR page 26 on how the ITMS did not have an internal supervisor over many years, and how it investigated a person hired to oversee their actions.

²⁶ CIR pages 5, and 33 to 36.

²⁷ CIR page 16.

²⁸ CIR page 29.

²⁹ There is evidence that this is happening to some departments, such as the State Department. See, for example,

Ronan Farrow. *War on Peace, The End of Diplomacy and the Decline of American Influence*. Norton, 2021

should be done in a controlled fashion to prevent the loss of essential functionalities.

³⁰ Karen Greenberg. *Subtle Tools*. Princeton University Press, 2021

THE NEW GOVERNMENT OPERATIONAL PROCEDURES described by Karen Greenberg³⁰ is yet another explanation for the potential government problems that allowed the ITMS misconduct to last for almost two decades. Greenberg argues on her book that since the 9/11 terrorist attacks, the US government crafted three “subtle tools”, that is, since then the US federal government began to: (1) leave aside established procedures and started to act without internal institutional constraints; (2) write new laws in a vague manner that provided the executive branch with an ample field of action; and (3) avoid the scrutiny of its actions, including internally, such as by creating new tribunals inside the executive branch to avoid the oversight of the judiciary branch or by restricting access to information to only a few members of congressional oversight committees. The ITMS case aligns well with the Greenberg’s analysis on the new forms of government operation. Overall, the ITMS was a division of the executive branch that eschewed the established guidelines of American intelligence agencies or police forces in order to obtain a vague mandate allowing it to act as it pleased, without a meaningful oversight of its actions or public acknowledgment. Indeed, the general public seems to be unaware that individual government agencies (such as the DOC’s Census in an example previously covered) can investigate them if they complain about their services on social media platforms. If Greenberg’s subtle tools are what allowed the emergence of the ITMS, it will be hard to prevent, detect, or fix the recurrence of the problems caused by the ITMS. Given the size of the US federal government, it is likely that a number of civil servants are already operating under vague mandates, without institutional constraint and with little oversight, and hence some agencies might be already behaving like the ITMS was. In this scenario, it would important to proactively search for such cases throughout government. Overall, dismantling the subtle tools is perhaps the safest way to preserve the well functioning of the federal government.

³¹ Michael Glennon. *National Security and Double Government*. Oxford University Press, 2014

THE TRANSITION OF THE US INTO A SECURITY STATE, as analyzed by Michael Glennon³¹, is a process that started under the Truman administration that is characterized by the transfer of power towards national security agencies. This is yet another potential institutional background configuration that allowed the abusive ITMS behavior to take place. In this line of thought, it is not the new forms of drafting and executing policy that lead to the ITMS problems but an internal re-balancing of power within the US government. Along these lines, it is worth noting the account of Rosa Brooks³² on how the Depart-

³² Rosa Brooks. *How Everything Became War and the Military Became Everything: Tales from the Pentagon*. Simon & Schuster, 2016

ment of Defense (DOD) is overtaking the mandate of other agencies since it is becoming one of the few efficient departments; the account of Ronan Farrow³³ of how the State Department lost ground to the Pentagon and intelligence agencies; the work of Radley Balko³⁴ on the militarization of the police force; the evidence collected by Daniel Golden on the growing influence of intelligence agencies on academic institutions³⁵; and the detailed analysis of Shoshana Zuboff³⁶ on the profound social transformation taking place with the rise of tech companies that are behaving evermore so as mass surveillance agencies. The problem here, when we focus on the ITMS case, is the potential for security states to become totalitarian. Following Hanna Arendt³⁷, what characterizes a totalitarian state is not the fact that they are powerful, but that they blur the distinction between the public and private lives. Arguing in this direction, strengthening the separation between the public and private spheres would be a crucial step towards preventing the types of problems caused by the ITMS. In this case, the paramount importance would be to strengthen and reaffirm the right to privacy and proper due process. In short, the main goal here is to prevent a totalitarian form of government by making sure that government agencies are not scouring the lives of citizens or carrying out clandestine operations against them.

IT IS WORTH CONSIDERING THE DRIVERS OF THE ITMS PRINCIPAL AGENT PROBLEM independent of the institutional shortcomings that enabled its occurrence. Anecdotal accounts of principal agent problems of intelligence agents seeking some personal gain from their position abound, and works of fiction capture their essence well³⁸. The CIR could benefit from a more detailed analysis of the personal gains of the ITMS agents, specially if it has a view towards understanding the motivations at the root of the ITMS rogue actions. For example, the CIR does not provide an account of the ITMS finances, or related revolving door issues, besides an overall account of the wasted government funds, running over a million dollars, caused by the ITMS investigation of the OES. Such an analysis, if it is ever carried out, would benefit from a detailed account of the companies hired by the ITMS, since there is ample evidence that many private intelligence agencies, driven to secure financial gains, are acting out of control³⁹.

The ITMS principal agent problems may have other root causes besides that of agents seeking to secure private career of financial gains. In line with the Specific Cases section above, the ITMS actions against DOC workers had a xenophobic and white supremacist bent. This type of problem is already present in law enforcement agencies⁴⁰. Here, we follow *A Field Guide to White Supremacy*⁴¹ and define the term to mean both the believe in the superiority of white people and the broad sys-

³⁴ Radley Balko. *The Rise of the Warrior Cop*. PublicAffairs, 2021

³³ Ronan Farrow. *War on Peace, The End of Diplomacy and the Decline of American Influence*. Norton, 2021

³⁵ Daniel Golden. *SPY Schools*. Picador, 2017

³⁶ Shoshana Zuboff. *The Era of Surveillance Capitalism*. Harvard University Press, 2019; and Shoshana Zuboff. *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*. *Organization Theory*, Volume 3, 1-79, 2022

³⁷ Hannah Arendt. *The Origins of Totalitarianism*. Harvest Book, 1967

³⁸ See, for example:

Florian von Donnersmarck. *The Life of Others (Movie)*. Buena Vista International, 2006

³⁹ Tim Shorrock. *The corporate take over of U.S. intelligence*. Salon, June 2007; Dana Priest and William Arkin. *A hidden world, growing beyond control*. Washington Post, June 2010. URL <https://www.washingtonpost.com/topsecretamerica>; Barry Meier. *Spooked - The Trump Dossier, Black Cube, and the Rise of Private Spies*. Harper, 2021; and Ronan Farrow. *Catch and Kill - Lies, Spies, and a Conspiracy to Protect Predators*. Back Bay Books, 2020

⁴⁰ FBI. *White Supremacist Infiltration of Law Enforcement*. FBI Intelligence Assessment, 2006; Alice Speri. *The FBI has quietly investigated white supremacist infiltration of law enforcement*. The Intercept, 2017; and Kathleen Belew. *Bring the War Home*. Harvard University Press, 2019

⁴¹ See, in particular, the chapter on anti-immigration of this reference.

Kathleen Belew and Ramón Gutiérrez. *A Field Guide to White Supremacy*. University of California Press, 2021

tems of inequality that insure racial disparity even without individual belief. The ITMS actions against people that commented on the Census on social platforms presumably have the same underlying motives. The reference above stresses the importance of not considering violent white supremacy acts as isolated events carried out by “lone wolves”. In this vein, considering the ITMS actions as acts of isolated misguided agents is a myopic approach to the problem. The account of the ITMS actions would add to the literature the fact that not even high-level accomplished US government workers are immune from the actions of white supremacists, and that intelligence units also have white supremacist problems. It further provides a window on how these actions are carried out. In particular, after failing to win court cases, it seems that the ITMS agents centered on sabotaging the carriers of minority workers. The account of the unnamed worker that was put under surveillance even while at home and forced to quit is particularly telling. It displays a close resemblance to “Zersetzung” operations carried out by the Stasi in order to isolate and undermine targeted people while keeping veil of normalcy and averting formal judicial procedures⁴². More precisely, the Stasi manual⁴³ says Zersetzung amounts first to the accumulation of detailed information on the target and then to the systemic degradation of reputation, image and prestige through the engineering of social and professional failures to undermine the self-confidence of individuals to switch them off, whereas the account of ITMS agents on the case being considered say that they spied on the private life of the targeted person over many years and then proceeded to place an enormous amount of pressure on the individual to isolate her at work (e.g. to make her “radioactive” using their words) and force her to quit her position. Both the Stasi and the ITMS applied their methods to individuals that they knew to be innocent but belonged to “undesirable” groups. These actions can lead to lasting changes to the lives of the target individuals⁴⁴, as is to be expected. There are potentially negative macro outcomes as well. The economy is ultimately not only based on enforceable contracts, but also on mutual trust⁴⁵. Acts like those perpetrated by the ITMS, or other white supremacist actions done by the government, may undermine the trust minorities have on society in general, leading to a persistent economic impact similar to the one felt to date by the actions of the Stasi⁴⁶.

⁴² Mike Dennis and Norman Laporte. *State and Minorities in Communist East Germany*. Berghahn Books, 2011

⁴³ Ministry for Security and State. *Dictionary of political and operational work (Zersetzung entry)*. 1985

⁴⁴ Anna Funder. *Stasiland: Stories from Behind the Berlin Wall*. Granta Books, 2003

⁴⁵ Kenneth Arrow. *Gifts and Exchanges*. *Philosophy and Public Affairs*, 1, 343-362, 1972

⁴⁶ Andreas Lichter, Max Löffler, and Sebastian Sieglösch. *The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany*. *Journal of the European Economic Association*, 19, 741-789, April 2021

Conclusion

This note provides a summary of a congressional Committee Investigation Report on abuses and misconduct at the Commerce Department. The report covers the actions of a division of the Department of Com-

merce, the ITMS, that evolved from a security group with a mandate to protect the department's building and director into an intelligence agency with police powers operating under minimal oversight. This led to a "principal agent problem", that is, the division's workers acted in accordance to their preferences in detriment to the public interest they were hired to represent. The abuses and misconduct of this division were not limited to the misuse of funds but included sabotage acts against people the division knew to be innocent and clandestine operations that violated fundamental rights such as the right to privacy. Ultimately, they seem motivated by white supremacist issues. The ITMS misconduct only took place and lasted for decades because of failures at a number of other government agencies. It is unclear if this was a systemic failure or a happenstance. This note considers three potential mechanisms that could enable the systemic failure of parts of government: (1) the rapid expansion or dismantling of federal government agencies; (2) the new government operational procedures triggered by the 9/11 terrorist attacks; and (3) the transition of the US government into a security state. Some proposals were also considered to counter these potential underlying issues, including some for tail-event cases. Since it is unclear if the ITMS rogue mode of operation was adopted by other government agencies, the development of policies and guidelines to prevent or mitigate it is not just an interesting academic topic but a timely research agenda in support of the well-functioning of government.

References

- Hannah Arendt. *The Origins of Totalitarianism*. Harvest Book, 1967.
- Kenneth Arrow. *Gifts and Exchanges*. *Philosophy and Public Affairs*, 1, 343-362, 1972.
- Radley Balko. *The Rise of the Warrior Cop*. PublicAffairs, 2021.
- Kathleen Belew. *Bring the War Home*. Harvard University Press, 2019.
- Kathleen Belew and Ramón Gutiérrez. *A Field Guide to White Supremacy*. University of California Press, 2021.
- Shawn Boburg. *Commerce Department security unit evolved into counterintelligence-like operation*. Washington Post, May 2021.
- Rosa Brooks. *How Everything Became War and the Military Became Everything: Tales from the Pentagon*. Simon & Schuster, 2016.
- US Congress. *Intelligence Reform and Terrorism Prevention Act*. December 2004.
- US Congress. *Committee Investigation Report - Abuse and Misconduct at the Commerce Department*. July 2021.
- Mike Dennis and Norman Laporte. *State and Minorities in Communist East Germany*. Berghahn Books, 2011.
- Ronan Farrow. *Catch and Kill - Lies, Spies, and a Conspiracy to Protect Predators*. Back Bay Books, 2020.
- Ronan Farrow. *War on Peace, The End of Diplomacy and the Decline of American Influence*. Norton, 2021.
- FBI. *White Supremacist Infiltration of Law Enforcement*. FBI Intelligence Assessment, 2006.
- Ministry for Security and State. *Dictionary of political and operational work (Zersetzung entry)*. 1985.
- Anna Funder. *Stasiland: Stories from Behind the Berlin Wall*. Granta Books, 2003.
- Michael Glennon. *National Security and Double Government*. Oxford University Press, 2014.
- Daniel Golden. *SPY Schools*. Picador, 2017.
- Karen Greenberg. *Subtle Tools*. Princeton University Press, 2021.
- Andreas Lichter, Max Löffler, and Sebastian Sieglöcher. *The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany*. *Journal of the European Economic Association*, 19, 741-789, April 2021.
- Barry Meier. *Spooked - The Trump Dossier, Black Cube, and the Rise of Private Spies*. Harper, 2021.
- Dana Priest and William Arkin. *A hidden world, growing beyond control*. Washington Post, June 2010. URL <https://www.washingtonpost.com/topsecretamerica>.
- Tim Shorrock. *The corporate take over of U.S. intelligence*. Salon, June 2007.
- Alice Speri. *The FBI has quietly investigated white supremacist infiltration of law enforcement*. The Intercept, 2017.
- Florian von Donnersmarck. *The Life of Others (Movie)*. Buena Vista International, 2006.
- Kimmy Yam. *After being falsely accused of spying for China, Sherry Chen wins significant settlement*. NBC News, November 2022.
- Shoshana Zuboff. *The Era of Surveillance Capitalism*. Harvard University Press, 2019.
- Shoshana Zuboff. *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*. *Organization Theory*, Volume 3, 1-79, 2022.