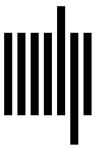
# Cryptographic City

## Decoding the Smart Metropolis

By: Richard Coyne

## Citation:

*Cryptographic City: Decoding the Smart Metropolis*
**By:** Richard Coyne
**DOI:** 10.7551/mitpress/14712.001.0001
**ISBN (electronic):** 9780262374811
**Publisher:** The MIT Press
**Published:** 2023



The MIT Press

# 11 Cyberattacks

One way to conceal information is to position it within a confusion of signals (that is, to obfuscate). Hash strings obscure the content of the files that they reference. Steganography, hiding one image inside another, obscures a secret image within the complexity of the carrier image that conceals it. A maze will obscure access to the center, the tower, the keep, or the gate to the city via the confusion of twists, turns, and junctions. Spatial confusion is one of the means of defense and protection in cities as in nature.

Confusing the perceptions of predators and prey is a basic device in species selection. Any single zebra will blend in with the herd when they stand together. It is harder to tell where one zebra ends and the next one starts. As they approach the herd, the visual field of a lion or hyena is assaulted with vertiginous to-and-fro movement—which is somewhat stroboscopic. Any predator will be confused, just enough, to give the herd time to take evasive action. Such momentary obfuscation buys time.[1] Obfuscation is a wily tactic exercised by both predator and prey. It is also a feature of accidental and deliberate human tactics of attack and evasion (figure 11.1). One of the strongest means of attacking an adversary, target, or victim is to throw them into confusion.

Markets, fairgrounds, malls, and busy supermarkets lure shoppers with sounds, colors, and spatial confusion to provide an entertaining melee. They also disorient shoppers as prey for sellers and advertisers. On the other hand, multiplication obscures the prey. A would-be thief will find it harder to identify a particular victim in a high-density neighborhood made up of hundreds of apartments than in a sparsely populated rural setting.

Factors other than protection contribute to spatial obfuscation in the urban context. The exteriors of buildings commonly conceal their functions.

**Figure 11.1**
Dazzle obfuscation. HMS *President* docked on the River Thames, London, as a recreational venue and painted to resemble tactics for camouflaging ships to confuse detection by adversaries. Photograph by Ron Ellis via Shutterstock.

A building designed with multiple readings in mind constitutes such a dissimulation. In the old part of Edinburgh there are recesses in external walls that are the same shape and size as windows. That is to preserve the regular patterns of openings across a wall, even where there's a chimney or fireplace on the inside that blocks the possibility of a window opening. Cities as sites of communication are populated by mimetic, faux, mock, and dissimulating architectural signs that occlude the legibility of the city. Obfuscation is also a prominent tactic for attack and defense in the online world, and hence in the cryptographic city.

Cryptography is a subspecies of obfuscation. After all, much encryption turns messages into apparent noise. Cryptography invokes an explosion of possible combinations designed to overwhelm the cognitive and computational capabilities of humans and computers to sift, sort, identify, and edit signals and messages.

## A Darker World

By some philosophical readings, the world is a mass of confusion, and clarity is the exception, imposed by sophisticated cultural framings, and language.[2] To obfuscate is "to confuse, bewilder, or stupefy," according to the OED. But the first definition is "to darken," from the Latin *obfuscare*. From a phenomenological reading, our perception of the world can usefully be considered as a process of revealing and concealing. As the spotlight of human perception and insight scans across the world it reveals certain objects, attributes, and ideas, but others recede into shadows and complete darkness. The world is already a sea of zebra stripes. It is our lionlike acuity in marking out the exceptional, the independent, and the adventurous that constitutes the unusual moment of lucid perception.

Obfuscation is effective as a tactic to confound the mind of the rational citizen. An intriguing book by Finn Brunton and Helen Nissenbaum outlines various obfuscating tactics and their remedies and ethics: *Obfuscation: A User's Guide for Privacy and Protest*.[3] Here, obfuscation is a way of dealing with information. It is semiotic. It pertains to information that we want to conceal. In the zebra case, the information is the location of one vulnerable, singular individual that is potential prey. For Brunton and Nissenbaum, "Obfuscation is contingent, shaped by the problems we seek to address and the adversaries we hope to foil or delay, but it is characterized by a simple underlying circumstance: unable to refuse or deny observation, we create many plausible, ambiguous, and misleading signals within which the information we want to conceal can be lost."[4] Their text is a handbook to help readers avoid the inadvertent disclosure of personal online data, including one's location, and other information by which advertisers, government and foreign agencies, political operatives, and hackers can surveil and profile us. The authors provide several means of obfuscating data.

## Jobsworth

Brunton and Nissenbaum show how you can obscure your actions and intentions by adhering to the letter of the law, to comply with formal requests, to do what you are told, and to deliver truthful information—and you can confound your antagonist by doing so. I think anyone who works

in a large organization knows how compliance can obfuscate, particularly in relation to information: provide the information requested—even more information than is asked for; provide it unfiltered and unsorted; inundate your antagonist with "paperwork" and keep it coming; exploit the fact that the requester may not really know, or forgets, what they are looking for or why they requested it. After all, you were only asked for the information, not to be helpful beyond that.

Here is a variant of this obfuscatory tactic. Brunton and Nissenbaum point to the use of vague language in a promise. It looks as though you are saying what people want you to say, but you say it in such a way that it provides you with a loophole in case you cannot deliver on your promise: "I promise to negotiate a deal that will deliver the best outcome." Is the promise to negotiate a deal, to deliver the best outcome, or both, and the best outcome for whom? That's my example. They provide the example of a web service that asserts, "Certain information may be passively collected to connect use of this site with information about the use of other sites provided by third parties."[5] That looks to be showing responsibility and care for user privacy, in that the website is telling you something. But it is confusing. What we would like to read is: "We do not collect user data," but they probably do. Unfortunately, they don't say that they do not.[6]

I particularly like Brunton and Nissenbaum's advice on spreading culpability to protect the guilty. So, activists in a group wear the same clothes as each other, including face coverings. Then it is harder for witnesses to identify the individual who actually threw the eggs at the politician, smashed the plate-glass door, or spray painted the shop window. An obvious variant is for the individual activist to appear indistinguishable from the innocent crowd. In fact, certain offences are best committed where there are crowds. If you are going to do something against the law, then look the same as everyone else. The "I am Spartacus" tactic is a variant. Only one person is guilty, but every member of the group or the extended group of sympathizers confess to the crime. Outside of despotic Roman "justice," they cannot all technically be guilty, or punished.

The identification and arrest of rioters after the U.S. Capitol security was breached on January 6, 2021, highlights the extent to which the proliferation of online photo sharing, live streaming, surveillance cameras, police body cams, and press coverage subverted the aims of individuals who wanted to get lost in a crowd.

Brunton and Nissenbaum's book is ostensibly about how citizens and activists can evade and subvert how commercial interests and governments collect data about them. But bad actors deploy the same tactics. In April 2019, the U.S. Department of Justice released a report on Russian interference in the U.S. presidential election of 2016, authored by a team led by Special Counsel Robert Mueller.[7] A witness in the Mueller investigation said that President Trump "took every step that he could to try to obfuscate, to try to get people to lie, tried to reward those people who refused to cooperate with a legitimate investigation, tried to punish and denigrate the people who were cooperative."[8] That is how one witness summarized the Mueller Report. I searched for "obfuscation" in the report and it's not there, but "obstruction" features prominently.

Brunton and Nissenbaum's book was published before Trump was elected, and before the concept of "Active Measures" gained currency among the general population. These were the operations of the Russian Internet Research Agency and of the GRU (General Staff of the Armed Forces of the Russian Federation) that include tactics to confuse, obstruct, and obfuscate. Brunton and Nissenbaum's book addresses different sides of such operations. On the one hand are powerful predators who want to exploit us and make money or extract political advantage from our personal information. On the other hand are those ordinary citizens and (apparently) good-faith activists who want to confound the attempts by powerful corporations, organizations, and states to monitor, surveil, profile, and coerce us.

Practitioners of cryptography want to both obscure secret messages and obscure the fact that there are secret messages. Codebreakers and hackers want to conceal that they have stolen or copied some data. They also want to conceal secret code and stegomalware they have inserted into digital assets and to cover their tracks, concealing that they were even there. Software platforms are difficult and confusing in any case with contributions from multiple players and under the control of operating systems, subroutine libraries, interface protocols, and networks that are in turn developed and maintained by a circle of independent suppliers. Software is an ideal medium in which to employ obfuscation and espionage.

## Automated Obfuscation

Brunton and Nissenbaum describe *chaff*, a technique to confound radar by scattering scraps of foil-backed paper into the sky. Chaff is a simple,

low-tech method to scramble radar signals to make it more difficult for an adversary to detect the location of your attack plane as it approaches its target. The point is not to hide the aircraft, but to make it appear there are more planes than there really are. That is a trick of obfuscation: not to hide, but to multiply, and thereby overwhelm the system of detection. Technologies are good at multiplying and repeating. Eventually the recipient of the obfuscation tactic gets the data they seek, but it takes time, even for detection technologies. As for a herd of zebra, obfuscation serves to delay rather than prevent detection.

There is a zebra versus lion, prey versus predator contest in play, as each vies against the other with ever more sophisticated means of evasion and capture. It is a basic contest played out over various scales of technological sophistication. Brunton and Nissenbaum provide many examples of the ploy by both good and bad actors, predators and prey, the powerful and the less powerful, the corporatized and the independent, the seller and the consumer, the saboteur and the victim.

The deployment of Twitter bots provides an obvious example of obfuscation by digital means. Fake twitter accounts generate new tweets. They retweet the tweets of others, select from catalogues of standard tweets, generate likes, and generate new fake accounts to compound and confuse social media messaging. Such tactics attempt to skew people's impressions toward a particular point of view, to exaggerate the apparent support for one opinion or person, or simply to confuse the audience. The Mueller Report made clear that bad actors seek both to conceal (obfuscate) their own operations and to obscure the public discussion by generating fake support for conflicting opinions. The adversary seeks to divide a population and sow chaos.

When the U.S. Department of Justice first made the Mueller Report available to journalists and the public it was released as an image file. Every page was a digital optical scan, but you couldn't search that for words or phrases. Whether deliberate or not, the format served initially as a means of obfuscation. Soon after its release I tried to run the file through Adobe's optical character recognition (OCR) function, but the file was too large for my version of the OCR reader at the time. Eventually, a week or so later, a searchable version of the report appeared online.[9] The use of technological impediments served as a means of further delay. As with encryption and

decryption methods, changes in software, standards, and systems impact tactics for obfuscation and breaking through the noise.

## Cyber Espionage

I have already alluded to how bad actors and agents of espionage might deploy obfuscation. The respectable-sounding Internet Research Agency (IRA) is a media organization that was started by the Russian government in 2013, initially to exert influence over Ukrainian and Russian citizens.[10] It has since rebranded and bears the name of its location in the landmark business center Lakhta in St. Petersburg. The 2021 U.S. NIC (National Intelligence Council) report into interference in the 2020 U.S. federal elections describes the organization as "The Kremlin-linked influence organization Project Lakhta and its Lakhta Internet Research (LIR) troll farm."[11] Before the 2016 U.S. presidential election the Russian IRA directed its operations to influence online political discussions in the United States, with further influence in other countries, though that hasn't drawn as much attention in the press. Reports released in 2018 referred to so-called "organic" online activity that included innocent content supplied by consumers as tweets, Facebook posts, blogs, and YouTube clips, as well as comments, reposts, links, likes, followings, and subscriptions.[12] So "organic" online activity embraces noncommercial consumer activity, in contrast to advertising activity paid for by sponsors that usually appears conspicuously as banner ads, pop-ups, inserts, and branded clips in news feeds and videos.

Advertisers seek to persuade and to reinforce a brand. Political parties and other interests deploy a range of tools of persuasion and for propaganda. They may also seed organic posts by legitimate audiences and customers. Organic customer engagement strategies enhance the reach of the brand with only modest financial outlay.

The reports I referred to earlier deploy the term *organic reach* to describe the processes by which advertisers or any organizations exert influence by pretending to be social media consumer sources. They deliver false consumer-led online activity such as recommendations, or just drop propaganda or endorsements into tweets, posts, videos, and online conversations. Covert and fake organic tactics of the kind deployed by the Russian IRA included posts, feeds, comments, and other content, including likes,

each delivered from false or misattributed accounts, organizations, communities, and individuals. A malign organization can introduce paid ads that deliver misinformation and that claim to be from a source other than those running the influence operation. Bots, algorithms, and pools of human operatives pretending to be legitimate social media users simulate organic activity and seed further reach.

So-called "voter suppression" was one of the tactics of Russia's Internet Research Agency to discourage people in the United States from voting. The tactic was directed at people on social media within a demographic that can be identified readily and is usually inclined to vote in a particular direction. For example, the average African American voter is or was assumed likely to vote Democrat in certain US states. To suppress that vote, the malign agent presents to members of that group "tweets designed to create confusion about voting rules," according to the report *Tactics and Tropes of the Internet Research Agency*.[13] Voters might be led to believe falsely that they can get someone else to vote on their behalf, or that they can deliver their vote online. The Russian IRA might also encourage that demographic to vote for a third-party candidate or an independent minority candidate, thereby diluting the support for a main party candidate. The third method here is to persuade members of that group not to vote as their vote will not make a difference anyway. That is one example of how such an externally generated influence campaign can work. Combined with sophisticated monitoring of social media users, targeted organic reach, and hacking into private records, we have the makings of cyber subversion, if not cyber warfare. Obfuscation serves as a means of espionage and it is among a series of measures by which foreign agents confound local, urban sociability and security in the cryptographic city.

## Active Measures

Political commentators identify how Russia's IRA deployed long-standing Cold War tactics to induce foreign targets to disclose secret information and to spy on operations in their own countries.[14] Active measures include well-resourced propaganda and influence campaigns operating across media channels including social media. Some techniques of "active measures" focus on *kompromat*, a variant of компромисс, the Russian word for "compromise," various means of accessing and activating embarrassing and

damaging information about individuals and groups. Not all active measures are effective all the time, but are cheap to implement and are much less costly than planes and artillery. In any case, if a tactic does not succeed, the main return is confusion among its adversaries. If such "active measures" are delivered by one government against another, and the malign government is an autocracy, then its state-controlled media cushions any bad publicity that comes its way. That malign government can also keep its operations hidden, as it infiltrates the global Internet and social media with propaganda and misdirection.

An illuminating article by Pawel Surowiec shows why active measures and kompromat are difficult to counter: "There is a risk that countering *Kompromat* inspired propaganda head on will lead to the proliferation of the very information one is trying to counter in cyberspace."[15] Cautious commentators will state that they don't want to restate the lies out loud as that increases their circulation. The article by Surowiec was published in Autumn 2017, the early months of the forty-fifth presidency, and events moved quickly: "*Kompromat* is a flexible and powerful concept. It enables denial (rarely apologia) of any wrongdoing when uncovered. Additionally, it often reveals falsehoods and lies about political or business opponents along with truthful negative information, blending accuracies and misinformation, thus allowing it to damage its targets in a highly sophisticated manner."[16] Kompromat obfuscates.

For those attracted to conspiracy theories, it is indeed peculiar that made-up stories about a "deep state" and the free press as "enemy of the people" had greater circulation than the more plausible, fascinating, and "real" narratives that identified the culpability of kompromat campaigns. But deflection from its own operations is also part of the kompromat play—the circulation of distracting and unsettling kompromat-inspired false accusations and conspiracy theories.[17]

## Zero-Day Attacks

The repertoire of malevolent active measures by states and criminal opportunists includes those that target cities. Cities and computer systems are complicated, with legacy components, new and old bits of code, tangled communication routes, and gateways and networks that make them vulnerable to bad actors and resourceful hackers. Overlay such digital vulnerabilities

onto the arcane and labyrinthine structures of cities and infrastructures that have grown piecemeal over time. That gives you the hackable city, a city that is victim of its own obscure legacies and substructures.

Some espionage tactics exploit complexities and vulnerabilities in computer systems. The concept of "zero-day vulnerabilities" emerged in the 2020s. It is usual for computer code to have "bugs," no matter the level of quality control and how well it is written. Any computer interaction, utility, or function depends on components supplied from a range of sources. Operating systems provide the environments in which programs function. Programmers draw on shortcuts to various functions such as libraries of subroutines. A weakness or incompatibility among any of these components introduces errors. From the point of view of an end user on a word processor or data entry package, the software may simply "crash," or a function may fail.

Thanks to online monitoring and harvesting of user feedback, software suppliers develop and distribute regular "patches" that fix or replace malfunctioning software components. That works as a means of maintaining software quality as long as the supplier finds out about the bug before it causes serious damage, including reputational damage to the supplier's product line.

Some malfunctions have implications that extend beyond inconvenience for a single end user. These are vulnerabilities that provide portals into software and systems for the spread of malware that cripples the digital functions not just for the individual using the software, but also for networks of users, organizations, countries, nations, and even global systems. According to cybersecurity lore, in the digital world it is safest to assume there are bad actors, operating alone or in groups dispersed across networks, who operate as rogue employees of government, or who belong to both benign and rogue states. All have the capacity to detect and exploit vulnerabilities in software.

We can also assume that there are many points of entry to any networked system. Software, such as the Microsoft operating system, is widely distributed. Not all individuals and organizations run the latest versions of the software or institute all patches and fixes when available. Vulnerabilities concentrate at the least secure nodes in such networks.

How do rogue agents identify these vulnerabilities? There are many methods. One obvious route for a hacker is to steal the source code

somehow and analyze it for potential failure in the event of bad input data that it cannot trap and that causes memory overflows, for example. But the most common method of attack is "fuzzing," "a brute force approach in which the attacker provides overly large or otherwise unanticipated inputs to a program and then monitors the response," according to an article on such vulnerabilities.[18]

Once the hackers know what makes the software system fail then they can hold the software to ransom for the users who depend on it, either by threatening to disable the software, or encrypting its data so that the company or user being targeted needs to pay for the key to restore it. This was the tactic in the case of the malware breach of the UK's National Health Service in 2017. The so-called *WannaCry* ransomware attack exploited vulnerabilities in the Microsoft operating system. The U.S. National Security Agency (NSA) had already detected the vulnerability and kept that knowledge secret in case they could exploit it as part of their own cybersecurity defense and attack weaponry.

Hackers had also come across the vulnerability, perhaps through a leak from the NSA or by some other means, and exploited it by disabling crucial systems and demanding payment in exchange for restoring the data. Software users were outraged by the hackers of course, but had the NSA reported the vulnerability to Microsoft, which would then have patched it, this would have spared the NHS and other organizations the ransomware scam. The NSA had nicknamed the Microsoft vulnerability "EternalBlue." Information scientist Stephen Wicker explains the problem: "Having learned of (or discovered) EternalBlue, the . . . perpetrators used the vulnerability to put target machines in the desired vulnerable state, and then issued a 'request data' command that caused an encrypted viral payload to be loaded onto the target machines. The payload included ransomware as well as software that searched for other machines that had the same vulnerability. The ransomware rapidly propagated across the Internet, infecting machines that shared the EternalBlue vulnerability."[19]

The offense does not stop with the data hack. Knowledge of vulnerabilities is a marketable commodity. Users, systems operators, or hackers may happen upon these vulnerabilities by serendipity, or may actively seek them out. Once detected, we might think it appropriate to report any vulnerabilities to the software supplier, which would then write code to obviate the problem and distribute that as patches or upgrades. That may take a

few days or weeks, during which time the security of the software and the systems that depend on it are compromised. There are *zero days* to fix the problem, hence the naming of the zero-day vulnerability.

Cybersecurity critic Nicole Perlroth explains the phenomenon of zero-days incursions into the functioning of major software systems: "They are a cloak of invisibility, and for spies and cybercriminals, the more invisible you can make yourself, the more power you will have. At the most basic level a zero-day is a software or hardware flaw for which there is no existing patch."[20] Cybersecurity advocates might argue that the security of citizens is served well by government agencies able to exploit vulnerabilities in the software and systems of hostile foreign actors. The information has value to the NSA or other state instruments that can exploit the vulnerabilities in disabling the systems of their adversaries.

As well as the software developers and suppliers, third parties are interested in knowing about the vulnerabilities. An online article by Matt Suiche in 2016 revealed that a group of hackers known as the *Shadow Brokers* detected the EternalBlue vulnerability and offered the information for online auction.[21] They might have sold that information to the NSA or perhaps the information was sourced from the NSA in the first place.

The infrastructures of entire cities have been compromised through ransomware exploits. Government security agencies have to deal with the question of whether they should disclose their knowledge of any vulnerabilities to the vendor, or keep it to themselves to aid their own covert operations.

### Bulk Surveillance

Nation states have departments such as the NSA and the UK National Cyber Security Centre that commit to keeping national communications networks and hence city infrastructures secure. They invariably deploy cryptography in both defensive and offensive measures. In 2013 one of the NSA's contract employees, Edward Snowden, disclosed NSA covert operations via the press in a series of consequential revelations. He was pursued by law enforcement and eventually moved to self-imposed exile in Russia. He explained his reasoning and psychological state in an autobiography, as well as several documentaries and press interviews.[22]

To provide an urban context, as a fugitive Snowden declared that when crossing a busy road, he instinctively looked away from oncoming traffic for fear of having his image captured on a dashcam.[23] People are more easily recognized face-on than in profile. That short observation from his book *Permanent Record* delineates some salient themes in the cryptographic city: surveillance, risk and paranoia.[24]

What he and other insiders exposed was that the NSA was able to obtain wholesale communications data from every citizen on the phone network in the United States and abroad. The initial revelation provided by Snowden to *The Guardian* and published on June 6, 2013, stated that for telephone communications the NSA covert operations accessed the phone numbers of both parties at either end of a call, with location data, unique identifiers, and the time and duration of calls.[25] The NSA was not requesting from the communications service providers the content of conversations, but the *metadata*. We normally think of secret service investigations as directed at key targets, but here the data of everyone on the telephone network was collected whether or not they were suspects. The data was stored in bulk on vast servers ready to be mined as needed. Software could trace links and detect patterns. The collection of metadata was automated, and no human being needed to ever see the data—unless authorized to investigate particular individuals. Here the security agencies obscured their engagement with the data by the claim that it is not the data they want to inspect but data about the data.

Snowden and others have argued that a great deal about a person's life can be harvested from such metadata, including networks of contacts, lifestyle, activities, and competencies. This information space is even more revealing if you include the bulk collection of email metadata, browser histories, debit card transactions, and travel data, especially if linked. Is it really surveillance if the metadata is collected in bulk and not inspected by a human operative?

A helpful blog post by information law lecturer Paul Bernal explains the problem of identifying when surveillance actually happens. There are three key moments: "the gathering or collecting of data, the automated analysis of the data (including algorithmic filtering), and then the 'human' examination of the results of that analysis of filtering."[26] Does surveillance happen when the bulk data is collected, or when humans inspect the data?[27]

Bernal argues that the same privacy question arises in the case of video surveillance: the moment the surveillance system is installed, when there's the means for someone (a relative, the landlord, an employer, a law enforcement official) to see what the camera sees, even if they never take up the opportunity.

## Urban Vulnerabilities

The risks caused by cyber espionage are consequential for cities and communities. The NSA headquarters is located between the cities of Washington, DC, and Baltimore. Among its many operations the NSA develops digital tools for spying on other countries and exploiting some of the vulnerabilities I have described. *Wired* magazine reported that "US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers."[28] But some of these tools leaked out, and around 2017 were turned on the city of Baltimore to cripple its infrastructure. According to a *New York Times* report, "For nearly three weeks, Baltimore has struggled with a cyberattack by digital extortionists that has frozen thousands of computers, shut down email and disrupted real estate sales, water bills, health alerts and many other services."[29] Many NSA workers live in Baltimore, so the NSA's hacking and counter-hacking operations rebounded onto those citizens.

The metaphor of *urban vulnerability as commodity* offers an interesting lens through which to consider city challenges. The nefarious exploitation of information about vulnerabilities that might result in failure of some kind recalls persistent urban scenarios of protection rackets, black markets, and insurance scams. Failure by a sports player is worth something to bad actors who rig games and sports that involve betting. Traders in stock markets benefit from insider knowledge about impending failure. In the worst cases such failure can be engineered, with or without the complicity of the protagonists.

As another disreputable practice, political parties and interests can put forward "spoiler" candidates who they know will fail to be elected, whose policies accord with some opposition voters and effectively splits them away from their support for the mainstream opposition. These candidates

are encouraged to run and are installed to fail and to dilute the opposition's vote.

There are also brokers who trade portfolios of failed urban enterprises, failed retail outlets, and unprofitable property investments. These put losses on the ledger and provide a way of avoiding corporate taxes in some countries. Disreputable competitive practices may induce failure in competing enterprises to facilitate takeovers. Once written off, products that fail in terms of profitability can be used to bulk up product portfolios and serve as lures within bargain offerings. Under this framing, wealth disparity, homelessness, and uneven access to technical and social infrastructures also constitute urban vulnerabilities readily exploited by negative and disruptive political agents—not to mention opportunistic agents who seek to profit from pandemics and other calamities.

I began this chapter with the tactics of obfuscation that are means for concealing data and fall within the repertoire of urban tactics deployed by state instruments, corporations, activists, and day-to-day providers and consumers of information. That led me to consider the wider challenges presented by cyber espionage, cyberattacks, ransomware, and other threats to urban citizens and infrastructures.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Coyne, Richard, author.
Title: Cryptographic city : decoding the smart metropolis / Richard Coyne.
Description: Cambridge, Massachusetts ; London, England : The MIT Press, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2022021507 (print) | LCCN 2022021508 (ebook) | ISBN 9780262545679 (paperback) | ISBN 9780262374811 (pdf) | ISBN 9780262374828 (epub)
Subjects: LCSH: Smart cities. | Internet of things. | Urban development—Data processing. | Public administration—Security measures. | Data encryption (Computer science)
Classification: LCC TD159.4 .C69 2023 (print) | LCC TD159.4 (ebook) | DDC 004.67/8—dc23/eng/20221011
LC record available at https://lccn.loc.gov/2022021507
LC ebook record available at https://lccn.loc.gov/2022021508

10 9 8 7 6 5 4 3 2 1