© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

CONTENTS

Tables ix

Figures xi

Abbreviations and Acronyms xiii

1 Intelligence Challenges in the Digital Age: Cloaks, Daggers, and Tweets 1

2 The Education Crisis: How Fictional Spies are Shaping Public Opinion and Intelligence Policy 16

3 American Intelligence History at a Glance: From Fake Bakeries to Armed Drones 44

4 Intelligence Basics: Knowns and Unknowns 77

5 Why Analysis Is So Hard: The Seven Deadly Biases 108

6 Counterintelligence: To Catch a Spy 143

7 Covert Action: "A Hard Business of Agonizing Choices" 169

8 Congressional Oversight: Eyes on Spies 195

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

9 Intelligence Isn't Just for Governments Anymore: Nuclear Sleuthing in a Google Earth World 225

10 Decoding Cyber Threats 251

Acknowledgments 277

Notes 281

Selected Reading 379

Index 393

For general queries, contact webmaster@press.princeton.edu

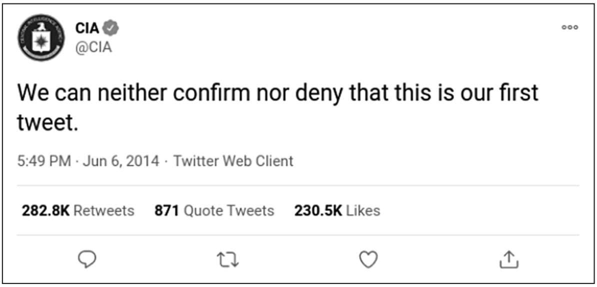
© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

1

INTELLIGENCE CHALLENGES IN THE DIGITAL AGE

CLOAKS, DAGGERS, AND TWEETS

IN JUNE 2014, I was scrolling through my Twitter feed when I came across the following Tweet:



CIA
@CIA

We can neither confirm nor deny that this is our first tweet.

5:49 PM · Jun 6, 2014 · Twitter Web Client

282.8K Retweets **871** Quote Tweets **230.5K** Likes

At first, I thought it was a joke. The Central Intelligence Agency (CIA) is notoriously secretive—so shadowy, even its public affairs officers don't always tell you their names. But the Tweet was real. America's cloak-and-dagger agency had finally joined the social media age. The Internet went wild. "Who knew?—they have a sense of humor," reported CNN.[1]

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

The CIA's Twitter debut was a light-hearted moment in a darkening landscape. New technologies such as artificial intelligence (AI), Internet connectivity, quantum computing, and synthetic biology are disrupting global economics and politics at unprecedented speed. Never before has the United States faced a more dynamic and dangerous world. For the CIA and the seventeen other agencies comprising the U.S. Intelligence Community (IC), this is a moment of reckoning.[2]

Artificial intelligence is transforming both commerce and defense in ways that could destabilize social orders and alter the global distribution of power. Computer scientist Kai-Fu Lee estimates that AI could eliminate up to 40 percent of jobs worldwide in the next fifteen to twenty-five years, in sectors ranging from trucking to the service industry.[3] AI is also poised to revolutionize how wars are fought—automating everything from logistics to cyber defenses to unmanned fighter jets that can sense and attack faster than humans.[4] As former Google CEO Eric Schmidt and former Deputy Secretary of Defense Robert Work wrote, "AI is accelerating innovation in every scientific and engineering endeavor."[5]

Not since electricity has a breakthrough technology ushered in so much potential promise and peril. Russian President Vladimir Putin has declared that whoever leads in AI development "will become the ruler of the world."[6] More than a dozen countries have launched national AI initiatives. And China has made no secret of its plans to become the global leader in AI by 2030, part of its strategy to challenge U.S. economic and military dominance.[7] American experts and policymakers are sounding the alarm. "We are in a strategic competition. AI will be at the center. The future of our national security and economy are at stake," noted the bipartisan National Security Commission on Artificial Intelligence in a 2019 report.[8]

AI isn't the only technology reshaping the world. Internet connectivity is supercharging politics, fueling protest movements like the Arab Spring and Hong Kong's Umbrella Movement, repressive crackdowns like China's persecution of the Uighurs, and Russian information warfare campaigns that reach deep into the societies of other nations. The

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

so-called Internet of Things (everyday devices with Internet connections) is spreading to billions of toys, cars, appliances, and more—and bringing cyber vulnerabilities with it.[9] Facebook algorithms are deciding what news we read and influencing how we think, enabling the manipulation of populations at scale.

There is greater upheaval still to come. In 2019, Google announced it had achieved "quantum supremacy"—a computing breakthrough so powerful that a math problem a supercomputer would need ten thousand years to solve could be cracked by its machine in just three minutes and twenty seconds. Experts likened it to the Wright Brothers' first flight: the dawn of a technological era opening vast new possibilities. Not all of them are good. Quantum computing could eventually unlock the encryption protecting nearly all of the world's data today.[10]

Synthetic biology is enabling scientists to engineer living organisms and create new ones not found in nature, with the potential for revolutionary improvements in the production of food, medicines, and data storage, as well as new weapons of war.[11] Because living cells are programmable like computers, they could eventually be engineered to make just about anything. Potential uses include manufacturing plastics, creating plants that can detect chemical munitions by changing color, and even designing bioweapons that target individuals on the basis of their DNA.[12] Here, too, Chinese military leaders have made innovation a top priority, calling biotech the new "strategic commanding heights" of national defense.[13]

The COVID-19 pandemic accelerated many of these trends, sending entire economies and societies online and fueling the use of biosurveillance technologies like smart jewelry that tracks symptoms[14] and data analytics that can identify which rooms of a building an infected person used and whether they were wearing a face mask.[15]

We've seen technological advances before. But never have we seen the convergence of so many new technologies changing so much so fast. This moment is challenging American intelligence agencies in three profound ways.

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

First, technological breakthroughs are transforming the threat landscape by generating new uncertainties and empowering new adversaries. During the Cold War, America had one principal enemy: the Soviet Union. The Cold War was a dangerous time, but it was simpler. America's top intelligence priority was clear. Every foreign policy decision was viewed through the lens of "What would Moscow think?"

Now, a wide array of bad actors is leveraging technology to threaten across vast distances. China is launching massive cyberattacks to steal American intellectual property[16] and building space weapons to cut off U.S. military satellite communications before the fighting ever starts.[17] Russia is using Facebook, Twitter, and other social media platforms to wage information warfare.[18] Three dozen countries have autonomous combat drones and at least nine have already used them.[19] Terrorist groups are using online video games to recruit followers[20] and Google Earth to plan their attacks.[21] Despots in developing nations are employing high-tech repression tools.[22] Weak states and non-state actors can inflict massive disruption, destruction, and deception with the click of a mouse.

For most of history, power and geography provided security. The strong threatened the weak, not the other way around. Oceans protected countries from one another, and distance mattered. Not anymore. In this era, the United States is simultaneously powerful and vulnerable to a head-spinning number of dangers, all moving at the speed of networks. It's a far cry from the plodding pace of Soviet five-year plans from a few decades ago.

The second challenge of the digital age involves data. Intelligence is a sense-making enterprise. Agencies like the CIA gather and analyze information to help policymakers understand the present and anticipate the future. Intelligence isn't always right. But it beats the best alternatives: guesswork, opinion, and gut feel.

In the old days, spy agencies in a handful of powerful countries dominated the collection and analysis of information. They were the only organizations with the resources and know-how to build

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

billion-dollar satellites, make and break sophisticated codes, and collect information at scale.[23] In 2001, the National Security Agency (NSA) intercepted about two hundred million foreign emails, phone calls, and other signals a day.[24] Few countries or companies could come close.

Now, data is democratizing, and American spy agencies are struggling to keep up. More than half the world is online,[25] conducting five billion Google searches each day.[26] Cell phone users are recording and posting events in real-time—turning everyone into intelligence collectors, whether they know it or not.[27] Anyone with an Internet connection can access Google Earth satellite imagery, identify people using facial recognition software, and track events on Twitter.

On January 6, 2021, when pro-Trump rioters violently attacked the U.S. Capitol to prevent congressional certification of the 2020 presidential election, causing the deaths of five people, online sleuths immediately started mining images and video posted on social media to help law enforcement agencies identify the perpetrators. One anonymous college student even created a website called Faces of the Riot. Using widely available facial detection software, the student scanned hundreds of videos and thousands of pictures shared by rioters and others on the social media site Parler and extracted images of those who may have been involved in the Capitol siege.[28]

The sheer volume of online data today is so staggering, it's hard to comprehend: in 2019, Internet users posted 500 million tweets, sent 294 billion emails, and posted 350 million photos on Facebook *every day*.[29] Some estimate that the amount of information on earth is doubling every two years.[30]

This kind of publicly available information is called *open-source intelligence* and it is becoming increasingly valuable. When U.S. Navy SEALs conducted their secret nighttime raid on Osama bin Laden's Pakistani compound, Pakistan's military didn't detect a thing. But a local information technology consultant named Sohaib Athar did. Hearing strange noises, he took to Twitter. "Helicopter hovering above Abbottabad at 1 A.M. (is a rare event)," he posted. Athar ended

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

up live tweeting the operation, including reporting when an explosion shook his windows.[31]

Similarly, when Russia invaded Ukraine in 2014, the best evidence did not come from spies or secretly intercepted communications. It came from selfies: time-stamped photos taken by Russian soldiers and posted on social media with Ukrainian highway signs in the background. Social media has become so important, even the consoles at America's underground nuclear command center display Twitter feeds alongside classified information feeds.[32]

That's not all. Commercial firms worldwide are launching hundreds of small satellites every year,[33] offering low-cost eyes in the sky to anyone who wants them.[34] Some satellite sensors have resolutions so sharp, they can detect manhole covers from space.[35] Others can capture images at night, in cloudy weather, or through dense vegetation and camouflage.[36] And constellations of cheap, small satellites are offering something new: faster revisit rates over the same location to detect changes over time. Already, commercial imagery and machine learning tools are enabling some of my Stanford colleagues to analyze North Korea's trade relationship with China by counting the number of trucks crossing the border in hundreds of images over the past five years.[37] Commercial imagery is becoming so valuable that the National Reconnaissance Office, the American agency that builds and operates spy satellites, is spending $300 million a year to buy it rather than just building satellites of its own.[38]

In short, data volume and accessibility are revolutionizing sensemaking. The intelligence playing field is leveling—and not in a good way. Intelligence collectors are everywhere, and government spy agencies are drowning in data. This is a radical new world and intelligence agencies are struggling to adapt to it. While secrets once conferred a huge advantage, today open-source information increasingly does. Intelligence used to be a race for insight where great powers were the only ones with the capabilities to access secrets. Now everyone is racing for insight and the Internet gives them tools to do it. Secrets still matter, but whoever can harness all this data better and faster will win.

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Secrecy and the Origins of Non-Denial Denials

The CIA's "We can neither confirm nor deny" response is part of the popular lexicon. While often used as a laugh-line in movies or on Twitter, that non-denial denial is real.[39] A CIA lawyer came up with it in 1975[40] when information about one of the agency's most highly classified covert operations leaked to the press.[41] The operation was code-named AZORIAN.[42] It involved billionaire Howard Hughes, a CIA ship posing as a commercial deep-sea mining vessel,[43] and a daring effort to hoist a sunken Soviet submarine—along with its nuclear missiles[44] and secrets[45]—from the bottom of the Pacific Ocean right as Soviet ships were passing by.[46] At the time, Cold War tensions were high, the risks of exposure were great, and reporters were barraging CIA officials with questions.[47] The agency did not want to be caught lying about what it was doing in the midst of Watergate, but it didn't want to reveal anything to the Soviets, either.[48] "We can neither confirm nor deny" has been used ever since.

The third challenge posed by emerging technologies strikes at the heart of espionage: secrecy. Until now, American spy agencies didn't have to interact much with outsiders, and they didn't want to. The intelligence mission meant gathering secrets so we knew more about adversaries than they knew about us, and keeping how we gathered secrets a secret, too.

Walk into CIA headquarters and you feel it. There's a gleaming white marble Memorial Wall covered with more than 100 stars, each denoting an intelligence officer who died in the line of duty.[49] A Book of Honor records their names, except for forty entries that have only blank lines.[50] For these CIA officers, service remains classified even in death.

Balancing secrecy and openness is an age-old struggle. Secrecy is vital for protecting intelligence sources and collection methods, as well as securing advantage. Openness is vital for ensuring democratic accountability. Too much secrecy invites abuse. Too much transparency makes intelligence ineffective.

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

In the digital age, however, secrecy is bringing greater risk because emerging technologies are blurring nearly all the old boundaries of geopolitics. Increasingly, national security requires intelligence agencies to engage the outside world, not stand apart from it.

It used to be that adversaries threatened from abroad and we could see them coming; military mobilization took time. Now they can attack privately owned critical infrastructure like power grids and financial systems in cyberspace—anytime, from anywhere, without crossing a border or firing a shot. In the twentieth century, economics and security politics were separate spheres because the Soviet-bloc command economies were never part of the global trading order. In the twenty-first century, economics and security politics have become tightly intertwined because of global supply chains and dramatic advances in dual-use technologies like AI that offer game-changing commercial and military applications. Until now, intelligence agencies focused on understanding foreign governments and terrorist groups. Today they also have to understand American tech giants and startups—and how malign actors can use our own inventions against us.

Securing advantage in this new world means that intelligence agencies must find new ways to work with private sector companies to combat online threats and harness commercial technological advances. They must engage the universe of open-source data to capture the power of its insights. And they must serve a broader array of intelligence customers outside of government to defend the nation.

These days, the National Security Agency isn't the only big data behemoth. Amazon, Apple, Facebook, Google, and Microsoft are, too. Although some companies have declared they will never use their technology for weapons, the reality is their technology already is a weapon: hackers are attacking computer networks through Gmail phishing schemes and Microsoft coding vulnerabilities, terrorists are livestreaming attacks, and malign actors have turned social media platforms like Twitter and Facebook into disinformation superhighways that undermine democracy from within.[51] American intelligence agencies have to find better ways to access relevant threat information held by these and other companies without jeopardizing civil liberties or firms' commercial success.

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Intelligence agencies need the private sector more for innovation now, too. Analyzing massive troves of data, for example, will increasingly depend on AI tools. Technological advances (like the Internet) used to start in government and then migrate to the commercial sector.[52] Now that process is reversed, with breakthroughs coming from large companies like Google and Nvidia and from startups like Ginko Bioworks and Dataminr. Instead of developing technologies in-house, spy agencies now have to spot and adopt them rapidly from outside. That requires talent as well as technology, and the private sector is cornering the labor market, too, offering compensation packages and cutting-edge computing facilities that are hard for government agencies (or universities) to match. Companies have been hiring away so many top AI professors (forty-one AI faculty left academia in 2018 alone), experts are worried there won't be enough left to teach the next generation of students.[53]

Engagement and collaboration with the private sector don't come easily. Distrust of American spy agencies has a long history with some dark chapters. In the 1970s, revelations that intelligence agencies had been spying on Americans, infiltrating dissident groups, and assassinating foreign leaders prompted outcries and congressional oversight reforms. More recent controversies include CIA drone strikes and secret NSA surveillance programs revealed by a former agency contractor named Edward Snowden in 2013.

In the summer of 2014, a year after the Snowden revelations hit the press, I held a cyber boot camp for congressional staffers that included a visit to a major Silicon Valley tech company. As we filed into the conference room, the tension was palpable. One tech executive told the group he viewed the U.S. government just like China's People's Liberation Army—as an adversary that needed to be stopped from surreptitiously penetrating his systems. Jaws dropped. An intelligence committee staffer rushed outside to call the boss and relay the news: they had a lot more repair work to do. NSA's surveillance programs had been authorized, but in the eyes of tech executives, they had broken faith by secretly gathering customer data and making companies look weak, complicit, or both.

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Intelligence agencies are still working hard to rebuild that trust. As the agency's first "neither confirm nor deny" Tweet went viral, Director John Brennan put out a press release explaining that he wanted a social media presence to "more directly engage with the public and provide information on CIA's mission, history, and other developments."[54] When secret agencies feel the need to engage and inform, you know times are changing. It's an important beginning.

As noted above, emerging technologies are also unleashing a whole new world of publicly available or open-source information—from Russian soldier selfies in Ukraine to satellite images of Chinese trucks in North Korea—that is challenging the primacy of secrets and the insight they provide. While open-source information has always been important, secrets have reigned supreme inside America's intelligence agencies. Not everything was secret, but secrets were everything. As former CIA analyst Aris Pappas noted, during the Cold War it was easy to slip into the attitude of "Gee, if they spent a trillion dollars to get this information, it must be a trillion dollars' worth of information."[55]

Technological breakthroughs are even challenging ideas about who counts as a decisionmaker. Until now, national security policy was the province of government. Important decisions were made by federal employees who wore badges, held security clearances, and knew how the Intelligence Community worked.

Not anymore. Increasingly, decisionmakers live worlds apart from Washington—making policy choices in living rooms and board rooms, not just the White House Situation Room. They are voters targeted by foreign influence campaigns to divide society and manipulate elections. And they are executives and employees working in technology companies where rewards come from inventing new products and finding new markets, not protecting society from nefarious uses and downside risks. Leaders in these companies may want no part of American national security policy or global politics, but their decisions unavoidably affect both.

In the digital age, business is not just business. Tech policy *is* public policy. Social media companies are deciding what presidential messages to the world can be blocked or shared. Software developers are affecting

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

how vulnerable their global products will be to cyberattack. Cell phone and messaging app executives are making encryption decisions that determine how dissidents can operate and how law enforcement agencies can combat terrorists.

Leaders on both sides of the Silicon Valley–Washington divide must navigate this new world together. They cannot do it without intelligence about how the threat landscape is shaping the development and use of new technologies and how new technologies are shaping the threat landscape.

Serving a broader set of decisionmakers requires much more than declassifying old intelligence reports and conducting business as usual. This was one of the chief lessons of 2016. During that election cycle, intelligence officials detected many facets of Russian interference and became so alarmed, they decided to warn the public. On October 7, the director of national intelligence and the secretary of homeland security took the unprecedented step of issuing a joint press statement. But almost nobody noticed.

Why? In part because it was written in intelligence-speak. Here are the first few lines:

> The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts.[56]

To intelligence insiders, the message was serious and clear. To the public, not so much.

That same day, the infamous *Access Hollywood* audiotape—in which Republican nominee Donald Trump boasted about how easy it was for him to sexually assault women—hit the news. Guess which got more attention.

In the 2020 presidential election, intelligence officials became more active and creative, making video public service announcements, issuing

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

more frequent press releases, and granting more media interviews.[57] One October video even included counterintelligence chief William Evanina and General Paul Nakasone, who led both the Pentagon's cyberwarriors and the super snoopers of the National Security Agency. Their message: election threats were real but their agencies were on the job.[58]

These steps have been important but insufficient. The 2020 video announcement, for example, received just 22,400 views on YouTube before election day.[59] Russia's state-run propaganda mill, RT America (formerly called Russia Today), had more than a million YouTube subscribers.[60] Meanwhile, intelligence itself became politicized, with Director of National Intelligence John Ratcliffe selectively using secrets and publicizing suspected Russian disinformation to support President Trump's campaign.

In the pages that follow, I hope to give readers a better understanding of intelligence as well as the challenges American spy agencies now confront. There are no easy answers, but one imperative is already evident: America's intelligence agencies must adapt or they will fail. The biggest surprise attacks in modern American history—Pearl Harbor,[61] 9/11,[62] and Russia's interference in the 2016 presidential election[63]—occurred because spy organizations did not change fast or fully enough to meet emerging threats. This juncture, too, requires dramatic change to harness new technologies better and faster than adversaries do.

This book draws on nearly thirty years of researching American intelligence agencies and advising the U.S. government; hundreds of interviews with current and former intelligence officials and policymakers; an undergraduate course I taught at UCLA; and focus groups I held more recently with high school and college students about what they wanted to learn about intelligence and why.

It's worth nothing that I am a visitor to the secret world of intelligence, not an inhabitant. Although I have served on the National Security Council staff and advised intelligence officials and policymakers, I have never worked inside an intelligence agency. I am a career academic who has examined spy agencies from the outside—looking at how they have evolved over time, why they have such a hard time adapting to new threats, and how they can improve. I often feel like an anthropologist

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

who travels to the far reaches of Washington, D.C., to observe the foreign cultures of a rare and secret clan of people called intelligence officers.

Being an outsider has both drawbacks and benefits. On the one hand, I cannot examine what the classified record actually says about pivotal intelligence events. I can only study what happened after the fact. On the other hand, an outsider's perspective can bring healthy skepticism and independence. I am freer to ask uncomfortable questions—and come to unflattering conclusions—than an insider would be.

Chapter 2 starts by examining the crisis in intelligence education and its costs. Most Americans, including policymakers, have little idea how America's intelligence agencies actually work. Instead, fiction has played an outsized role. Years ago, a poll of my students led to a startling discovery: spy-themed entertainment seemed to be influencing attitudes on intelligence in significant ways. This chapter follows the trail, examining my national polling project, tracing the dramatic rise in "spytainment," and examining how Hollywood has fueled conspiracy theories and influenced policymakers from Supreme Court justices to soldiers on the front lines.

Chapter 3 covers American espionage from eighteenth-century invisible ink to twenty-first-century spy satellites. That may seem like a long time, but compared to the rest of the world, American intelligence history is quite short. George Washington's spies didn't come around until two thousand years after Chinese general Sun Tzu wrote his treatise on the use of intelligence in warfare, *The Art of War*. Today's vast intelligence enterprise emerged largely after World War II and reflects the country's evolving role in the world.

Chapter 4 covers intelligence basics. We examine what intelligence is, what it isn't, and how it operates—with a bird's-eye view of the decade-long hunt for Osama bin Laden and personal reflections by intelligence officials of their daily lives, ethical dilemmas, and best and worst moments.

Chapter 5 examines intelligence analysis and why it's so hard. From China's surprise attack in the Korean War to the mistaken reports around Iraq's weapons of mass destruction, analytic failures have

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

common causes. Chief among them are what I call the seven deadly biases, or the cognitive traps that can lead even the smartest minds astray. We also explore the coming world of artificial intelligence, discussing which kinds of analysis machines can do better than humans and humans can do better than machines.

Chapter 6 turns to one of the most sensitive points for the Intelligence Community: traitors. What motivates trusted insiders to become turncoats? How can intelligence officers recruit spies in the digital age, and how can they identify possible double agents while still maintaining the trust necessary to do their work?

Chapter 7 explores covert action, what former CIA Director Leon Panetta once called "a hard business of agonizing choices."[64] We start in the deserts of Yemen, where an American citizen and infamous terrorist named Anwar al-Awlaki was killed in a covert drone strike without a trial, judge, or jury. We explore what exactly covert action is and why all presidents use it even though it so often fails. And we walk through one of these agonizing choices, examining a hypothetical covert action dilemma from different perspectives.

In chapter 8, we examine the contentious world of congressional oversight—how it's developed, why it matters, why it rarely works well, and what the future holds. We also delve into debates over the CIA's detention and interrogation program and the NSA's warrantless wiretapping program, two of the most heated oversight controversies in intelligence history.

Chapter 9 turns to nuclear sleuthing in the digital age. Thanks to the Internet, commercial satellites, and automated analytics, nuclear intelligence isn't just for superpower governments anymore. We trace the rise of the new nuclear sleuths—individuals and organizations outside of governments who are transforming how illicit nuclear activities are tracked. This new ecosystem highlights the dramatic changes in intelligence emerging today, including opportunities and risks.

Chapter 10 concludes with cyber threats—what they are, how they have evolved, what they mean for intelligence, and the key challenges they raise. In many ways, cyberspace is the ultimate cloak-and-dagger battleground, where nefarious actors employ deception, subterfuge, and

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

advanced technology for theft, espionage, information warfare, and more. Cyber threats are hacking both machines and minds. This is only the beginning: artificial intelligence is creating deepfake video, audio, and photographs so real, their inauthenticity may be impossible to detect. No set of threats has changed so fast and demanded so much from intelligence.

For America's Intelligence Community, the digital age is filled with complexity and challenge. From catching traitors and undertaking covert action to understanding nuclear threats and operating in cyberspace, success requires a fundamental rethink about how to secure advantage in a radically new world. It starts by getting back to basics and depoliticizing intelligence again. But success also includes a mission shift that embraces open-source intelligence, develops new capabilities for both secret activities and open engagement, and rewards officials for doing things differently.

As we'll see, adapting to this technological era is an enormous paradigm shift. But it's essential.

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

INDEX

Note: page numbers followed by *f* and *t* refer to figures and tables respectively. Those followed by n refer to notes, with note number.

academic study of IC, 35–36, 299–300n125, 299n121

Afghanistan: bin Laden escape to, after 9/11, 99; Clinton administration policy on, 272; covert action in, 63, 100, 104, 174, 184; drone strikes in, 175; intelligence gathering in, after 9/11, 100; search for al Qaeda in, 100; Soviet occupation of, 178, 181, 183–84; as terrorism stronghold, 183

Afghanistan War: CIA and, 192–93, 246; and counterinsurgency doctrine, 192; and Manning documents, 31; Obama and, 179; and operation to kill bin Laden, 181; and regime change, 176

AI. *See* artificial intelligence

Alexander, Keith, 262

Alphabet. *See* Google

al Qaeda: interrogation of leaders of, 100–101; origins of, 183; and planning of 9/11, 37, 69; post-911 campaign against, 99–101, 170, 186; search for, in Afghanistan, 100; in Yemen, 170. *See also* bin Laden, Osama

“alternative competing hypotheses” process, 133

Amazon: and big data, 8; Prime, spytainment on, 25; refusal to cooperate with government, 276

American Protective League, 59

Ames, Aldrich, 150, 154, 155, 157–60

analysis of intelligence data: asymmetric information and, 113–15; coloring of, by personal experience, 105, 122–23; data shortages and, 111–13; deception and, 104, 116–17; failure of, in Korean War, 109–10; and general difficulty of predicting future, 111; and mental shortcut errors, 117–18; in search for bin Laden, 103–5; and success or failure, lack of feedback on, 115–16; superforecasting analysis techniques, 137–39

analysis, improvement of, 131–39; artificial intelligence and, 139–41, 235–36; format of information and, 134–36, 135*f*; identifying bias, ineffectiveness of, 131; Structured Analytic Techniques to force re-perception, 131–34; superforecasting techniques and, 137–39; testing of methods for effectiveness, 136–38. *See also* biases, and data analysis

Angleton, James Jesus, 160–64

Apple: and big data, 8; and encryption of data, 222–23; founding of, 121; influence on U.S. policy, 75; refusal to cooperate with government, 222–23

Arnold, Benedict, 44, 52, 54, 155

artificial intelligence (AI): challenges created by, 2; and competition for advantage, 141; and deepfake audio and video, 223, 243–46, 268; and improved data analysis, 139–41, 235–36; limitations of, 140; obstacles to

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

artificial intelligence (AI) (*continued*) adoption of, 140–41; professors of, leaving for industry, 27

The Art of War (Sun Tzu), 45, 79

asymmetric information: and analysis of intelligence data, 113–15; as barrier to congressional oversight of IC, 207–12

availability bias, 122–23

al-Awlaki, Anwar, 31, 169–71, 337n10, 347n161

AZORIAN, operation, 7

Baer, Robert, 92

Bash, Jeremy, 103, 104

Bay of Pigs operation (1961), 64, 174, 182

Bearden, Milt, 184

Bennett, Gina, 91–92, 93, 94, 95, 96

biases, and data analysis, 117–30; availability bias, 122–23; confirmation bias, 103–4, 118–21; framing biases, 126–29; fundamental attribution error, 123–24; groupthink, 129–30; identifying bias, as insufficient remedy, 131; mental shortcut errors, 117–18; mirror imaging, 124–26; optimism bias, 121–22. *See also* analysis of intelligence data

bin Laden, Osama: CIA plan to capture, 69, 205; escape from Tora Bora, 99; long search for, 98, 99–103; near capture of, after 9/11, 99; pre-9/11 intelligence on, 69, 205; role in 9/11 attacks, 79; and U.S. laws against assassination, 191

bin Laden, killing of, 78, 106–7; analysis of intelligence data, 103–5; choice of covert action for, 105–6, 320n159; and deniability, 181; intelligence leading to, 77–78, 86, 100–102; as intelligence success, 21; and open-source intelligence, 5–6; secrecy surrounding operation, 94; uncertainty of identification, 77, 102, 104–5; *Zero Dark Thirty* film about, 27–28

biology, synthetic, challenges created by, 3

Black, Cofer, 171, 214

Black Chamber, 46, 59–60, 304n13

Black Tom explosion, 58

Bletchley Park codebreakers, 46

Bond, James, 23, 26

Brennan, John, 10, 89–90, 120, 122, 195

British intelligence: history of, 46, 304n11; in U.S., 58

Bureau of Military Information, 56–57

Burr, Aaron, 53

Burr, Richard, 225*f*

Bush, George H. W., 177, 189

Bush, George W.: on assessments of Iranian nuclear program, 229; and covert action, 186, 192; and cyberattack on Iranian nuclear facilities, 264; drone strikes authorized by, 175, 343n91; National Security Council meetings, 73; and search for bin Laden, 91, 100; and September 11th terrorist attacks, 171

Cambridge Spies, 154, 162

Capitol riot (January 6th, 2021), 5, 39, 365n10

Carter, Ashton, 224, 257–58

Carter, Jimmy, 106, 177–79

case (operations) officers, duties of, 145–46

Casey, William, 183, 344n105

Castelnau, Noël de, 121

Castro, Fidel, 63, 171, 182

Center for Nonproliferation Studies, 225, 239

Center for Strategic and International Studies, 241, 247

Central Intelligence Agency (CIA): and Afghanistan War, 192–93; Angleton as counterintelligence chief at, 160–64; annual family day, 94; black sites, 18, 196–97; breech of computer system, 167–68; and congressional investigation of harsh interrogations, 195–98, 348n7, 349n24, 350n25; courting of positive portrayals in films and TV, 26–28; creation of, 46, 49–50, 63, 172; domestic spying by, 83; functions of, 63–64, 65, 72, 74, 82; headquarters, described, 7, 16, 148; and Korean War, 108–10, 114, 125, 322n22; lack

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

of oversight before 1970s, 201–2; and Libyan nuclear weapons, 229; Memorial Wall, 7; military's opposition to, 65; overemphasis on secrecy, 34; phone security at, 93; post-9/11 analysis reforms at, 133; pre-9/11 failures of, 34, 69, 115, 205; public relations efforts, 9; scandals of 1970s, and introduction of oversight, 202–5; and search for bin Laden, 101, 102–3; social media use, 1, 9; subcultures within, 92–93; as top-tier agency, 74, 311n130. *See also* counterterrorism interrogation methods; covert action by CIA; drone strikes by CIA

Chambliss, Saxby, 195, 220

Child, Julia, 62

China: and AI, 2, 141; censorship in, 85, 275–76; COVID-19 disinformation campaign, 243, 266; cyberattacks, 4, 261–62; destruction of U.S. spy network in, 166–68; domestic spying by, 83; establishment of Communist government in, 112; and great power competition, 75, 177; intelligence cooperation with Russia, 166; Internet disinformation campaigns, 243; Internet influence campaigns, 266–67; Julia Child in, 62, 62*f*; monitoring of, 79, 80, 112; Nixon and, 157; and nuclear weapons, 227, 228, 230, 235, 238, 242–43; open-source intelligence on nuclear weapons, 235, 238, 242–43; persecution of Uighurs, 2; and quantum computing, 223; satellites operated by, 250; Silicon Valley views on, 9; spying on U.S., 141, 146–47, 154–55, 165; stealing of U.S. military secrets, 147, 261–62; technological advances of, 2, 3, 4, 141; trade, open-source information on, 6. *See also* Korean War

Church Committee, 66, 174–75, 203, 220, 346n135

CIA. *See* Central Intelligence Agency

Civil War, U.S. intelligence in, 55–57

Clancy, Tom, 23–24

Clapper, James, 49, 72, 87–88, 91, 210–12, 253, 262, 367n26

classified information: and academic study of IC, 35–36; archaic rules on, 31; and derivative classification, 295n89; as necessary, 29; as obstacle to cyber operations, 296n92; outdated system for, 30; and overclassification, 29–31, 33, 297–98n102; and reclassification, 31–32; and special access programs (SAPs), 49; three levels of classification, 29; and underclassification, 33

classified information breaches, 11, 31. *See also* Ames, Aldrich; Hanssen, Robert; Lee, Jerry Chun Shing; Manning, Chelsea; Pollard, Jonathan; Snowden, Edward; spies; spying against U.S.; WikiLeaks

Cline, Ray, 186

Clinton, Bill, 41–42, 73, 89, 191, 272

Clinton, Hillary, 41–42, 300n130

Cloonan, Jack, 41

Coats, Dan, 86, 89, 98, 233, 261

Cohen, David, 253

Colby, William, 61, 151, 163, 189, 190, 202

Cold War: CIA covert action during, 174, 176, 180, 186; end of, and IC's failure to adapt, 205–6; Soviet disinformation campaigns in, 266; and U.S. intelligence, 48

computer modeling, uses of, 236

computer systems, cyberattacks' damage to trust in, 269–70

confirmation bias, 103–4, 118–21

Congress, annual intelligence threat hearing, 39, 73

congressional oversight of federal bureaucracy: effectiveness of, 206, 207; fire alarm and police patrol models of, 206–7; help from outside interests, 208

congressional oversight of IC: abuses and, 66; CIA time spent responding to, 350–51n34; committees' lack of budget power and, 218–20; Congress's awareness of poor quality of, 214–15; and covert action,

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

congressional oversight of IC (*continued*) 190–92, 346–47n151, 346n146; creation of dedicated committees for, 204; era of routinization (1970s–1990s), 202; era of strategic weakness (1990s–now), 205–6; era of undersight (1770s–1970s), 201–2; failures of, post-9/11, 206; fire alarm type of, 207; good, characteristics of, 199–200; information asymmetry and, 207–12; as inherently difficult, 198; investigation of harsh interrogations, 195–98, 348n7, 349n22, 350n25; lack of expertise and, 216–18; lack of reelection benefits for oversight committee members, 212–15; as not mentioned in Constitution, 199; partisanship and, 220–21, 356n129; police patrol type of, 207; poor, characteristics of, 200; secrecy as barrier to, 207–12; and September 11th terrorist attacks, 205–6; technological advances and, 221–24; term limits on oversight committee positions and, 216–18, 217*f*, 218*f*; three eras of, 200–206; underlying factors affecting, 198

conspiracy theories, 300n130; Internet and, 37–38; public's belief of, 37, 38–39; spytainment and, 36–40

Coolidge Committee, 29

coordination of U.S. intelligence: asymmetric information and, 114–15; Director of National Intelligence and, 70–73; failures of, before 9/11 attacks, 69, 205; ongoing problems with, 73–74; push for, 61, 63, 65, 70; reports recommending (1991–2001), 67–69, 68*t*; resistance to, 67, 71

CORONA satellite program, 232–33

Cotton, Tom, 43

counterintelligence: Chinese destruction of U.S. spy network, 166–68; defensive, 148–51; definition of, 145; and excessive mistrust, 160–64; and excessive trust, 156–60, 164; increased difficulty in digital age, 164–66, 167–68; methods used in, 145; offensive, 151–53; screening of employees as, 149–51; spies, capture of, 143–44

counterterrorism interrogation methods: congressional investigation of, 195–98, 348n7, 349n24, 350n25; defenders, arguments of, 197; destruction of videotapes of, 210; public's lack of interest in, 21; in search for bin Laden, 100; spytainment's influence on support for, 19, 22–24, 40–43; and *Zero Dark Thirty* film, 27–28

covert action by CIA: in Afghanistan, 63, 100, 104, 174, 184; assassination as, 22, 64, 76, 171, 174–75, 189; bin Laden killing as, 105–6; in Brazil, 64; in Chile, 174, 202; in Cold War, 174, 176, 180, 186; in Congo, 64, 175; congressional oversight of, 190–92, 346–47n151, 346n146; in Cuba, 63, 64, 174; defining characteristics of, 172–73; and democratic accountability, 185; as distraction from other CIA functions, 193–94; in early years, 63–64; efficacy of, 182–84; fig leaf and, 181; in Guatemala, 63, 174; in Iran, 63, 174, 176, 183, 184; in Iraq, 174, 175, 176, 192; in Italy, 64, 174, 180; and military action, blurring of line between, 192–94; moral issues in, 97, 184–89; and "neither confirm nor deny" response, 7, 284n39; in Nicaragua, 63, 174, 182–83; non-covert versions of, 175–77; number conducted, 64; as outside original CIA mandate, 63–64. 65; in Pakistan, 175, 176–77, 179; in Panama, 188–89; and plausible deniability, 172–73, 180–81, 190, 343n100; presidential support for, 172, 177–81; procedures for authorizing, 190–92; *vs.* secret action, 339–40n35; in Serbia, 174, 369n52; in Somalia, 175, 176–77; and targeted killing, rules for, 191, 346n143; types of, 171–72, 173–75; and unintended consequences, 183–84; as unique in U.S. government, 74; within U.S., as illegal, 173; against U.S. anti-war

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

protesters, 202–3; usefulness of, 179–81; in Vietnam, 63; in Yemen, 31, 169–71, 175, 176–77. *See also* drone strikes by CIA
COVID-19: Chinese disinformation campaign on, 243, 266; and Chinese espionage, 147; and increased use of technology, 3
crowdsourcing, uses of, 236
Cuba: covert action by CIA in, 63, 64, 174; missile crisis and, 116, 125–26, 228, 230, 246, 265–66, 326n79; spying on U.S., 146–47, 150, 168
Culper spy ring, 50–52, 306n37
culture of secrecy in IC, 33–35
"Curveball" (German source), 70, 120, 130
cyberattacks: and attribution problem, 259; deceiving attacks, 265–69; definition of, 254; demands on intelligence due to, 269–73, 276; destroying attacks, 263, 264; deterrence, difficulty of, 259; difficulty of determining purpose of, 270–71; disruptive attacks, 263; evolution of threats and U.S. policy, 256–60; five types of, 261; four countries primarily responsible for, 261; greater vulnerability of advanced countries to, 256; hacking/spying attacks, 262–63; and inevitable weaknesses in code, 271; instant response required to defeat, 272–73; as issue for companies and general public, 276; number of Internet users affected by, 260; potential for physical damage from, 257; real-time intelligence needed for, 271–72; stealing attacks, 261–62; by teenagers, 260–61; and trust in information, damage to, 269–70; U.S.-Israeli attack on Iranian nuclear facilities, 226, 263, 264; variety *vs.* quantity of, 273. *See also* Russian interference in 2016 election
cyber capabilities, U.S., focus on intelligence over attack in, 273–74
Cyber Command, U.S., 260, 271–72, 274, 296n92
cyberspace, as inherently insecure, 255
cyber warfare: as often subtle and diffuse, 258–59; Russian election interference as, 253, 254; by U.S., 369n52

data: critical importance in modern world, 254–56; cyberattacks' damage to trust in, 269–70; encryption, as issue, 222–23; fast and accurate analysis, strategic value of, 6; shortages of, as inherent in intelligence analysis, 111–13
data, increasing volume and availability of: and artificial intelligence, value of, 139–41, 235–36; challenges created by, 4–6
dead drop, 143–44, 152, 153, 306n37
deepfake audio and video, 223, 243–46, 267–69
Deep State, as conspiracy theory, 38–39
defectors, false, 161, 162
Defense Department: and Chinese nuclear weapons, 242; and classification of nuclear weapons data, 32; constant cyberattacks on, 262; and covert action, 173, 185, 193; cyber missions, 258–60, 273–74; cyber vulnerability, 262; establishment of, 63; Google's refusal to work for, 275; intelligence agencies, 71, 72, 73–74, 73*f*; and Iraq War, 120; and plausible deniability, 181; public affairs office, 26; study of espionage by Americans, 154, 155
Defense Intelligence Agency (DIA): creation of, 66; functions of, 74, 82; as top-tier agency, 74, 311n130
democratic accountability: covert action and, 185; tension between secrecy and, 49–50
devil's advocates, to test analysis, 133
DIA. *See* Defense Intelligence Agency
digital technology, and increased damage from spying, 164–66, 167–68
director of central intelligence, 65
Director of National Intelligence (DNI): creation of, 70–71; functions of, 72–73; Office of, 47, 49; weakness of, 71–72

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

disinformation campaigns online, 8, 265–69, 365n10, 373n113. *See also* deepfake audio and video; Russian interference in 2016 election

DNI. *See* Director of National Intelligence

domestic spying: legal constraints on, 75, 83–84; post-9/11 support for, 211; violations of constraints on, 9, 20–21, 83, 203, 204

Donovan, William “Wild Bill,” 60–61

drone strikes by CIA: controversy surrounding, 39–40, 75, 169–71; non-covert counterparts, 176–77; secrecy of, 31; use by past three presidents, 175

Dulles, Allen, 61, 288n21

EAGLE CLAW, operation, 178

Eisenhower, Dwight D., 190, 230

election of 1948, 111

election of 2016, 111. *See also* Russian interference in 2016 election

election of 2020: disputed results of, 39; interference in, 11–12; online disinformation campaigns in, 266–67

employees of IC: on best and worst moments, 97–98; bond among, 156–60, 317n86; daily life of, 93–95; ethical dilemmas and, 95–97; examples of, 90–92; isolation of, 33; return flights for those killed, 98

encryption, advances in, 222–23

Energy Department, intelligence unit, 74

Espionage and Sedition Acts of World I, 20, 58

ethical dilemmas, 95–97

Evanina, William, 12

Facebook: al Qaeda propaganda on, 170; and Americans’ ignorance about news, 21–22, 170; and big data, 8; and disinformation, 8; doctored videos on, 243–44, 267–68; failure to prevent misuse, 275; foreign influence campaigns on, 243, 251–53; influence on U.S. policy, 75; and interference in 2016 election, 251–54, 266; manipulation of public opinion, 3; and Russian information warfare, 4, 251–53, 257, 266, 274; senators’ ignorance about, 223–24; volume of traffic on, 5. *See also* Zuckerberg, Mark

“The Family Jewels,” 203

Farook, Syed Rizwan, 222–23

Federal Bureau of Investigation (FBI): and Apple encryption, 222–23; creation of, 58, 308n73; domestic spying by, 83; functions of, 74; Hoover’s efforts to promote, 26; overemphasis on secrecy, 34–35; pre-9/11 failures of, 34, 69, 205–6; and September 11th terrorist attacks, 115, 205–6; in World War I, 58–59

Feinstein, Dianne, 195–96

Fifteen Axioms for Intelligence Analysis (Watanabe), 124

Five Eyes partners, 146

Flournoy, Michèle, 259–60

framing biases, 126–29

Franklin, Benjamin, 50, 52, 53, 54

Freedom of Information Act (FOIA), difficulty of getting documents through, 35, 296n94, 298–99nn115–118

fundamental attribution error, 123–24

Gaddafi, Moammar, 176

Gates, Robert, 71, 89, 163–64, 181, 272

generative adversarial networks, 268

Geospatial intelligence (GEOINT), definition of, 74. *See also* National Geospatial Intelligence Agency

Goodfellow, Ian, 268

Google: and big data, 8; and deepfake technology, 268; and encryption of data, 222; influence on U.S. policy, 75; NSA monitoring of, 20; and open-source intelligence, 84; powerful tools available on, 5; and quantum computing research, 223; refusal to cooperate with U.S. military,

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

275–76; searches, *vs.* intelligence information, 85; Sketchup modeling program, 240; and supercomputing, 3; support for Chinese censorship efforts, 275–76; and technological innovation, 9; terrorists' use of, 4; volume of traffic on, 5

Google Earth, 4, 5, 226, 234, 247

Gordon, Susan, 75, 88, 98, 141, 255, 275

groupthink, 129–30

Gulf War, First, 124, 272

Hale, Nathan, 50, 51, 53

Hamilton, Lee, 208, 209, 215, 218

Hanssen, Robert, 143–44, 146, 151, 152–53, 154, 164, 165

Haplerin, Morton, 185

Harman, Jane, 71, 209–10, 220

Hayden, Michael, 21, 43, 89, 152, 190, 210, 212, 214, 218, 264, 274

Hecker, Siegfried, 240

Helms, Richard, 61, 89, 284n45

history of intelligence, early, 45–46

history of U.S. intelligence, 46–76; Americans' aversion to standing army and, 47; in Civil War, 55–57; in Cold War, 48, 64; in early Republic, 47, 54–55, 201; fragmented organizations, development of, 48–49; in Iraq War, 18, 37, 70, 105, 119–21, 130; in Korean War, 108–10, 112, 113, 116–17, 119, 122, 125, 322n12; on-again, off-again development of, 46–48, 55–57, 59–60; Pearl Harbor attack and, 60–63; in Revolutionary War, 44–45, 50–54, 117, 306n43; and tension between democracy and secrecy, 49–50; in War of 1812, 55; World War I domestic intelligence, 57–60

Homeland (tv show), 24, 36–37

Homeland Security Department, functions of, 315n36

Hoover, J. Edgar, 26

House Permanent Select Committee on Intelligence (HPSCI), 204, 216–18, 218*f*, 220, 221. *See also* congressional oversight of IC

Hughes, Howard, 7, 284n39

human intelligence (HUMINT): in Afghanistan, after 9/11, 100; betrayals by U.S. agents and, 144, 166; CIA collection of, 65, 72, 74, 82, 92, 193; decline in, after Cold War, 66; Defense Intelligence Agency collection of, 82; in Korean War, 110; underfunding of, in 1990s, 205

HUMINT. *See* human intelligence

Hussein, Saddam, 37, 105, 120–21, 130, 176, 228–29, 272

Hyten, John, 30, 33

IC. *See* Intelligence Community, U.S.

India: conflict with Pakistan, 227; and Korean War intelligence, 110; nuclear test (1998), U.S. failure to anticipate, 125, 228; and Russian disinformation, 266

information warfare: China and, 266–67; definition and terms for, 365n10; efforts to counter, 274; foreign influence campaigns on social media, 243, 251–53; Russian information warfare on social media, 2, 4, 223, 243, 251–53, 257, 266–67, 274. *See also* Russian interference in 2016 election

Inglis, Chris, 270, 272–73

Instagram. *See* Facebook

intelligence: as complex and specialized, 82–83; definition of, 79–80; gaining advantage as goal of, 75, 79; and known and unknown information, 80–82, 81*t*; many uses of, 79; ongoing importance of, 11; separation from policy-making, 87–90, 316n52; as tailored analysis, 85–86; as term, 314n21; twenty-first century threats and issues for, 75–76

Intelligence Authorization Act of 1991, 172

Intelligence Community, U.S. (IC): and adaptation, need for, 12, 15; and adaptation, obstacles to, 141; agencies in, 73–74, 73*t*; budgets of, 47, 82, 314n30; call to expand customer base to private sector, 274–75; courting of positive portrayals in films

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Intelligence Community, U.S. (IC) (*continued*)
and TV, 25–28; cultures and subcultures within, 92–93; fragmented organization of, advantages and disadvantages of, 48–49; growth of, 46–47; as loose federation of agencies, 66; and military, blurring of line between, 192–94; political impartiality of, 87–88; post-Cold War budget cuts, 66–67; public's lack of knowledge about, 17–22, 22*t*; and public trust, importance of, 43; size of, 82; and speaking truth to power, 85–86; top-tier agencies in, 74, 311n130. *See also* coordination of U.S. intelligence; employees of IC
Intelligence Reform and Terrorism Prevention Act of 2004, 70–71
intentions, predicting: difficulty of, 81–82; and fundamental attribution error, 123–24; by projection, 124–26
Internet: and breech of CIA computer system, 167–68; challenges created by, 2–3; and conspiracy theories, 37–38; and public access to open-source information, 234–35; and vulnerability to attack, 8. *See also* social media
Internet of Things, 2–3, 271
Internet Research Agency (IRA), 251
interrogation. *See* counterterrorism interrogation methods
Iran: bin Laden's son under arrest in, 102–3; covert action in, 63, 174, 176, 183, 184; cyberattacks by, 261, 263, 266–67; hostage crisis, 178; hostage rescue efforts, 64, 106, 178, 180; Internet influence campaigns, 243, 266–67; Iran-Contra affair, 182–83, 344n105, 346–47n151; monitoring of, 72, 79, 89, 121, 225–26, 239–40, 248; nuclear weapons program, 112–13, 225–26, 229–30, 231, 239–40, 263, 264; offensive cyber operations against, 226, 263, 264, 269; Shah, U.S. support for, 183; spying on U.S., 146–47; use of drones, 282n19
Iraq: covert action in, 174, 175, 176, 192; drone strikes in, 175; and Gulf War, 157, 272; Iraq Survey Group, 120; monitoring of, 124; Saddam bomb hoax, 244–45; use of drones, 282n19; and U.S. Iraq Liberation act of 1998, 176
Iraq War: and counterinsurgency doctrine, 192; and extremists on Internet, 273; faulty intelligence leading to, 18, 37, 70, 71, 76. 80, 105, 119–21, 130, 209, 229; and fundamental attribution error, 124; and groupthink, 130; intelligence analysis reforms following, 128–29, 136, 231; and Manning documents, 31; news coverage of, 215; Obama and, 179; and regime change, 176; U.S. policy in, 87; U.S. resources tied down in, 264
Israel: cyberattack on Iranian nuclear facilities, 226, 263, 264; former intelligence officers, and Psy-Group, 267; intelligence on Middle Eastern nuclear programs, 231, 238–39; OPEC and, 132–33; spying on U.S., 146; and ticking time bomb situation, 41; use of drones, 282n19; war against, as U.S. concern, 227

Jay, John, 53
Johnson, Jeh, 253, 367n26
Joint Special Operations Command (JSOC), 193
Justice Department: and American Protective League, 59; and CIA, 46; and espionage cases, 20, 59, 195–96, 262; FBI as part of, 74, 311n130; and Noriega, 188–89

Karber, Phillip, 242–43, 247
Kennan, George, 184–85
Kennedy, John F., 66, 88, 116, 126, 182, 190, 246
Kent, Sherman, 80, 81*t*, 127–28, 128*t*
Khrushchev, Nikita, 116, 126, 228, 246, 326n79
Kim Jong-Un, 113, 116, 256, 269, 362n68

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Korean War: and fundamental attribution error, 124; Soviet involvement in, 180–81; U.S. intelligence failure in, 108–10, 112, 113, 116–17, 119, 122, 125, 322n12
Kuklinski, Ryszard, 95
al-Kuwaiti, Abu Ahmed (al Qaeda courier), 86, 100–102

Lee, Jerry Chun Shing, 154–55, 166, 167
Lewis, Jeffrey, 239, 242, 362n68
Libya: intelligence assessments of, 121; Israeli intelligence on, 231; relinquishment of nuclear weapons, 229; terrorist attack by, 176; U.S. air strikes on (1986), 176; U.S. regime change efforts, 176
Lumumba, Patrice, 175

MacArthur, Douglas, 108–10, 113–14, 122, 124, 125
machine learning, uses of, 235–36
Madison, James, 50, 199
Mallory, Kevin, 154, 165
Manning, Chelsea, 31, 165
Martin, Hal, 165
McCain, John, 219
McLaughlin, John, 93, 105, 116
McMaster, H. R., 85
media, publication of Snowden's stolen documents, 20
Microsoft: and big data, 8; founding of, 121; influence on U.S. policy, 75; quantum computing research, 223; and vulnerabilities, 8, 271, 272
Military Intelligence Division (MID; G2), creation of, 57
mirror imaging, 124–26
misinformation. *See* disinformation campaigns online
Mohammad, Khalid Sheikh, 100–101
Morell, Michael, 27, 67, 91, 93, 94, 105, 194, 199
Moynihan, Daniel Patrick, 29–30, 67
Mueller, Robert, 260, 267
Müller-Lyer illusion, 131, 132*f*

Nakasone, Paul, 12, 260
National Counterintelligence Strategy, 147
National Counterterrorism Center (NCTC), 16–17, 104, 105
National Geospatial-Intelligence Agency (NGA): and automated analytics, 235–36; functions of, 74, 82; and hunt for bin Laden, 101; and information sharing, 241; place in intelligence community, 73, 73*f*, 311n130
National Intelligence Estimates (NIEs), 119; and Cuban missile crisis, 125–26; and Iran, 229–30; and Iraq, 128–29
National Reconnaissance Office (NRO), 6, 48–49, 74, 101, 311n130
National Security Act of 1947, 63, 64, 65, 83, 172
National Security Agency (NSA): creation of, 65; director of, as head of Cyber Command, 274; domestic spying by, 83, 211–12; and encryption, 222; functions of, 21, 65, 74, 82; hacking tools, theft of, 165–66; headquarters, counterintelligence measures at, 149; public relations efforts, 34; public's lack of knowledge about, 20–21, 22*t*; public support for, spytainment and, 23; and search for bin Laden, 99, 101, 102; Snowden's release of classified documents from, 9, 20–21, 165, 211, 222; as top-tier agency, 74, 311n130; volume of data collected, 4; and warrantless wiretapping, 18, 96, 289n32
"neither confirm nor deny" response, 7, 284n39
NGA. *See* National Geospatial-Intelligence Agency
9/11 Commission, 70, 115, 191, 205–6, 211, 215
9/11 terrorist attacks (2001): al Qaeda's planning of, 37, 69; al-Awlaki and, 170; and bin Laden, targeting of, 186, 191; bin Laden's escape following, 99; botched opportunities to detect, 69; causes of IC's failure in, 205–6; changes to intelligence agencies following, 16–17, 47, 70–71, 82,

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

9/11 terrorist attacks (2001) (*continued*) 105, 133, 192, 199, 206, 211–12; CIA desire to avenge, 171; CIA renditions after, 175; conspiracy theories on, 17, 37; intelligence failure prior to, 34, 68–69, 98, 115, 205–6, 211, 272; intelligence on bin Laden prior to, 69, 205; as one of biggest intelligence failures in U.S. history, 12; poor coordination within IC and, 67–69, 115; and U.S. concerns about Iraq, 124. *See also* bin Laden, Osama

Nixon, Richard M., 89, 157, 202

Nolte, William, 205

Noriega, Manuel, 186–89

North Korea: censorship in, 85; cyberattacks by, 256, 261, 263; cyberattacks on, 165; and nuclear weapons, 86, 109, 112–13, 227, 228, 236, 240, 247–48; open source data on, 6, 10, 236, 240, 247–48; poverty in, 109; program to share information on, 241; shortage of data for analysis of, 112–13, 116; Trump's dismissal of intelligence on, 86, 89; U.S. cyberattacks on, 256, 269. *See also* Kim Jong-Un; Korean War

NRO. *See* National Reconnaissance Office

NSA. *See* National Security Agency

nuclear intelligence: four categories of, 228; IC success in, 228–31; as once limited to government agencies, 227–28; tendency for overcorrection in, 231

nuclear intelligence by civilians: ability to share information, 240; advantages over government form, 238–41; and alerting of adversaries to security vulnerabilities, 247–48; automated analytics and, 235–36; availability of satellite imagery and, 232–34; characteristics *vs.* government form, 236–38, 237*t*; effectiveness of, 225–27; evaluation by IC, as distraction, 246–47, 249; high level of expertise in some groups, 248; impact of global proliferation of, 249–50; important role of, 248–49; Internet access to open-source information and, 235; need for standards, 250; people and organizations engaged in, 227, 236–37; and risk of correct but damaging information, 246, 249; and risk of deliberate deception, 243–46; and risk of incorrect information, 241–43, 249; successful analyses by, 238–40; value to U.S. intelligence, as still unclear, 249

nuclear weapons: China and, 227, 228, 230, 235, 238, 242–43; as existential threat, 227; India's nuclear test (1998), U.S. failure to anticipate, 125, 228; Iran and, 112–13, 225–26, 229–30, 231, 239–40, 263, 264; Libya and, 229; North Korea and, 86, 109, 112–13, 227, 228, 236, 240, 247–48. *See also* nuclear intelligence

Obama, Barack: ban on harsh interrogation methods, 42; on Bin Laden raid decision, 77–78; on Brennan, 122; and Chinese cybertheft, 262; and covert action, 31, 177, 179, 186; drone strikes authorized by, 31, 170, 175, 343n91, 347n161; on human rights, 179; and killing of bin Laden, 77–78, 97, 102, 104, 106–7, 107*f*; National Security Council meetings, 73; and rules for targeted killings, 346n143; and Russia's 2016 election interference, 253

ODNI. *See* Director of National Intelligence (DNI)

Office of Naval Intelligence, 57

Office of Strategic Services (OSS), 60–61, 161

Olson, James, 95, 97, 144, 146, 152, 160, 164

"Olympic Games" cyberattack. *See* Iran, offensive cyber operations against; Stuxnet

open-source intelligence (OSINT): increasing importance of, 82; increasing volume of, 5–6; leveling of intelligence playing field by, 84; as most common type, 19–20, 84–85, 288n21; and nuclear intelligence, 235, 238–40, 242–43; public access to, through Internet, 234–35

optimism bias, 121–22

For general queries, contact webmaster@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

OSINT. *See* open-source intelligence
OSS. *See* Office of Strategic Services

Pabian, Frank, 240, 241, 245
Pakistan: conflict with India, 227; and Libyan nuclear program, 229; and plausible deniability, 181; search for bin Laden in, 99–100, 101, 103; U.S. drone strikes in, 175, 176–77, 179; use of drones, 282n19. *See also* bin Laden, killing of
Palmer raids, 59
Panetta, Leon, 42, 72, 97, 100–104, 106, 171, 173, 189, 192, 257, 320n159
Pappas, Aris, 10, 95, 97–98
Parler, 5
Pearl Harbor attack, 60–63
Pentagon. *See* Defense Department
Petraeus, David, 192
Phillips, Bill, 90–91, 92, 93, 94–95, 96–97, 160
Pollard, Jonathan, 146
Polyakov, Dmitri (TOP HAT), 157–58
polygraph tests, 149–51, 151*t*
presidents: support for covert action, 172, 177–81; tensions with IC, 88–90, 98
probabilities, humans' poor understanding of, 122–23
Psy-Group, 267
public opinion: lack of knowledge about IC, 17–22, 22*t*; low estimation of IC ethics, 95; Psy-Group and, 267; views on IC, influence of spytainment on, 18–19, 22–24
Putin, Vladimir, 2, 38, 89–90, 253–54

quantum computing, 3, 223

Ratcliffe, John, 12, 89
Reagan, Ronald W., 176, 182–83, 188–89
Red Scare, first, 59
red teams, to test analysis, 104, 105, 130, 132
renditions, 175
Revere, Paul, 50
Revolutionary War, U.S. intelligence in, 44–45, 50–54, 117, 306n43
Rice, Condoleezza, 64, 127
Roberts, Pat, 214–15
Rockefeller, John D. IV, 191, 209
Rodriguez, Jose A., Jr., 210
Roosevelt, Franklin D., 60
RT (formerly Russia Today), 12, 253, 266
Rumsfeld, Donald, 30, 71, 80
Russia: and AI, 2; and Cuban missile crisis, 116; cyberattacks, 261, 262–63, 266, 366n23; domestic surveillance in, 83; and great power competition, 75; history of censorship in, 45, 83; information warfare by, 2, 4, 223, 243, 251–52, 257, 266–67, 274; intelligence cooperation with China, 166; invasion of Ukraine, 6, 10; and nuclear weapons, 227, 228; RT propaganda and, 12, 253, 266; and Saddam bomb hoax, 244; spying on U.S., 143–44, 146–47, 150, 152–53, 154, 155, 157–58, 165; technological advances of, 4; U.S. spying on, 157–58, 162–63; and World War I, 57. *See also* Putin, Vladimir
Russian interference in 2016 election: accusations of Republican collusion in, 43; facets of, 253; goals of, 253; IC's pre-election statement on, 11–12, 367n26; investigation of, 267; media's failure to cover, 11; as one of biggest surprise attack in U.S. history, 12; ongoing investigation of, 269; spreading of disinformation, 259, 266–67; through social media, 251–54, 252*f*, 257, 266; Trump and, 38; U.S. failure to respond to, 12, 274

satellite imagery: history of, 232–34; training required to interpret, 241–42
satellite imagery, commercial: and civilian surveillance of nuclear sites, 225–26, 232–34; image quality of, 6, 233–34, 237; impact of global proliferation of, 250; increasing availability of, 6, 234, 283n34
SATs. *See* Structured Analytic Techniques
Scalia, Antonin, 42

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

scenario planning, 132–33
Schiff, Adam, 268–69
Schlesinger, James, 163, 203
Schmidt, Eric, 2
SCIFs. *See* Sensitive Compartmented Information facilities
secrecy: as barrier to congressional oversight, 207–12; and daily life of IC employees, 93–95; IC's overemphasis on, 34–35; *vs.* openness, need for balance in, 7–8; tension between democracy and, 49–50; and unclassified information, 34–35. *See also* classified information
Secret Service, 57–58
security clearances: number in U.S. with, 30, 49, 149; time required to process, 149; trust among colleagues with, 156–57, 317n86
security *vs.* liberty, balance of, as issue, 75–76
Senate Select Committee on Intelligence (SSCI), 204, 215, 216–17, 217*f*, 220–21. *See also* congressional oversight of IC
Sensitive Compartmented Information Facilities (SCIFs), 148–49
SIGINT. *See* signals intelligence
signals intelligence (SIGINT): Civil War and, 56; Clapper and, 91; and counterintelligence, 168; NSA and, 21, 65, 74, 82; post-Cold War budget cuts and, 66–67; and war on terrorism, 99
"signal-to-noise" problem, 61
Silberman-Robb Commission (WMD Commission), 70, 120, 130
Silicon Valley–Washington divide, 9–10, 11, 221–23, 275–76
Snowden, Edward, 9, 20–21, 165, 211, 222
social media: foreign government disinformation campaigns on, 243; information warfare on, 4, 8; manipulation of information by, 3, 10; refusal to cooperate with government security efforts, 275; and Russian interference in 2016 election, 251–54, 252*f*, 257, 266; volume of open-source intelligence on, 5–6. *See also specific platforms*
SolarWinds cyberattack, 262–63, 269
speaking truth to power, 85–86
special access programs (SAPs), 49
special forces, U.S., 99, 106
spies, terminology for, 145
spying, on friendly countries, 146
spying against U.S.: by China, 147, 261–62; countries engaged in, 146–47; damage done by, 144, 147, 157–58, 166
spytainment (spy-themed entertainment): impact on real policy, 40–43; influence on public attitudes about IC, 18–19, 22–24; influence on support for harsh interrogation methods, 22–24, 40–43; and overestimation of IC power, 36–37; popularity of, 24–25
SSCI. *See* Senate Select Committee on Intelligence
State Department, Bureau of Intelligence and Research, 74
STRATCOM. *See* Strategic Command
Strategic Command, U.S. (STRATCOM), 148
Structured Analytic Techniques (SATs), 133
Stuxnet, 264
Sulmeyer, Michael, 260
superforecasting analysis techniques, 137–39
synthetic biology, challenges created by, 3

technological advances: challenges created by, 2–9; and congressional oversight of IC, 221–24; monitoring of, as new focus for IC, 8–9. *See also* quantum computing; satellite imagery
technology companies: de facto setting of public policy by, 10–11, 75, 276; and encryption, 222–23; government/IC's need to work with, 9, 75, 257, 276; IC efforts to build trust with, 10; prioritizing of innovation over national security, 10, 222–23; refusal to cooperate with IC or

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

military, 9, 222–23, 275–76; talent pool, monopolization of, 9
Tenet, George, 67, 69, 70, 87, 92, 133, 146, 191, 193, 205, 229
Tetlock, Phil, 115, 128, 137–39
ticking time bomb scenario, 41–42
TOP HAT. *See* Polyakov, Dmitri
traitors: capture of, 143–44, 146, 152–53, 167; demographic characteristics of, 155; methods of communication with, 152, 332n43; motives of, 153–55, 156*f*; surveillance of, 152
Truman, Harry S., 49–50, 63, 64, 65, 75, 174
Trump, Donald J.: *Access Hollywood* tape, 11; conflict with IC, 86, 89–90; and Deep State, 38–39; drone strikes authorized by, 175, 177; and election of 2020, 12, 39; impeachments of, 39; and January 6th Capitol riot, 5, 39; Twitter feed of, 84–85
Turner, Stansfield, 178, 179
twenty-first century intelligence, threats and issues for, 75–76
24 (film): influence on policy, 40–42; and popularity of spytainment, 24; and public opinion on torture, 19, 40
Twitter: access to, 5; CIA public relations on, 197; CIA's first Tweet on, 1–2; and civilian monitoring of nuclear programs, 226; and disinformation, 8; and hackers, 260–61; influence on U.S. policy, 75; and interference in 2016 election, 266; and killing of bin Laden, 5–6; and Russian information warfare, 4, 252–53, 266, 274; senators' confusion about, 223; Trump and, 84–85; volume of traffic on, 5

underwear bomber, 170

VENONA, 161
voters, foreign campaigns to influence, 10. *See also* election of 2020; Russian interference in 2016 election

war, AI and, 2, 281n4
War of 1812, U.S. intelligence in, 55
Washington, George, 44–45, 50–55, 117, 201, 265, 306n43
waterboarding, 19, 21, 22–23, 40, 41, 197, 350n25
Watergate break-in, 202, 203
WikiLeaks, 11, 31, 253
Willoughby, Charles, 110, 114, 119, 122, 323n40
Wilson, Woodrow, 58, 59
WMD Commission (Silberman-Robb Commission), 70, 120, 130
Woolsey, James, 89, 157, 334n76
Work, Robert, 2
World War I: optimism bias in, 121; U.S. domestic intelligence in, 57–60
World War II: British intelligence in, 46; U.S. and, 47–48
wrong-side-of-maybe fallacy, 128
Wyden, Ron, 211–12

Yahoo: cyberattack on, 260; and encryption of data, 222; NSA monitoring of, 20
Yemen: al Qaeda in, 170; covert action in, 31, 169–71, 175, 176–77
Yoo, John, 41
YouTube: al Qaeda propaganda on, 170; Russian disinformation on, 12, 252; volume of traffic on, 266; warning about election interference on, 12
Yugoslavia, Soviet invasion of, 127–28

Zero Dark Thirty (film), 27–28
Zuckerberg, Mark, 223–24, 244, 267–68, 275

For general queries, contact webmaster@press.princeton.edu