17 Reflections on the future of intelligence

Gregory F. Treverton

Introduction

This chapter reflects on my experiences in government, in both policy and intelligence positions, drawing especially on my recent tenure as Chair of the US National Intelligence Council (NIC).¹ It assesses challenges for the future of intelligence, many of which have long been with us but are newly reconfigured: balancing tactical and strategic intelligence; building and adjusting stories in a shapeless world; dealing with transparency and big data; finding new ways to add value; intelligence as an argument for policy; breaking the tired intelligence cycle and dealing with new competitors who are also potential colleagues.

That would have been my list of challenges had Donald Trump not been elected president. Yet here, too, as in almost every aspect of US policy, the Trump administration scrambled the deck, injecting enormous uncertainty. Its malfeasance raised three additional challenges: reinvigorating a demoralized workforce; reorienting domestic intelligence, and last, and most worrisome, dealing with a world in which truth is personal or subjective, and, indeed, the very idea of truth is under attack. Thus, this chapter begins with the challenges as I might have portrayed them in more normal times, then concludes with reflections on my puzzlement about how lasting and how momentous the distinctly non-normal times of the Trump administration will prove to be.

Balancing strategic and tactical

An enduring challenge for the Intelligence Community is balancing the urgent need for actionable tactical intelligence with the need for too often-neglected strategic intelligence. The hand wringing about the primacy of urgent tactical intelligence over strategic has characterized all my years as a student, consumer and sometimes practitioner of intelligence. This issue is made all the worse by the shapelessness of the current world, which means that every crisis must be approached afresh on its own terms. This is especially heightened by the nation's hypersensitivity to the threat of terrorism, which poses a minimal threat to the United States homeland but is hardly perceived that way by the public – or so characterized by politicians (Malley and Finer 2018).

DOI: 10.4324/9781003164197-24

From my perch at the NIC, this acute sensitivity to terrorism was doubly deforming of our work. When we looked at Nigeria, there was not much Nigeria: it was Boko Haram. Instead of focusing on the complexities facing Nigeria, Africa's largest economy and highest population, we solely focused on a terrorist group in Nigeria's north. And even when we looked at Boko Haram, there was not much Boko Haram: it was all deciphering networks and targeting bad guys. We all wondered and worried, where do these people come from, and why are they doing what they're doing? Although we did what we could at the NIC trying to understand root causes and motivations, we were only scratching the surface of Boko Haram, let alone Nigeria.

In 2016, the NIC produced about 700 pieces of paper. More than half of those were memoranda that were set in motion by the deliberations of the two main policymaking bodies in the administration – the Principals Committee, comprised of the relevant cabinet secretaries, or, more often, the Deputies Committee, comprised of their deputies or number threes. These memoranda were produced in response to “taskings” by the National Security Advisor, one of her deputies, or another senior National Security Council official, and were used as the focal point for assessing options and teeing up decisions. Not all those papers were purely tactical. Some were the “what ifs?” of the sort that should be the warp and woof of intelligence-policy relations: “if we do x, how will Putin respond?” Because we were at all the policy meetings, we knew what was going on. Yet as Chair of the NIC, my task, every day, was to find the time and capacity not only to answer the questions policy officials asked but also to answer the more strategic ones they weren't asking.²

The perils of focusing on the tactical at the expense of the strategic run through many episodes of American foreign policymaking

A prominent example is the decision to arm Islamic mujahideen resistance during the Soviet Invasion of Afghanistan. Although America's decision ultimately led to the Soviet Union's eventual retreat from Afghanistan, it also empowered radical Islamic elements, some of which later became the Taliban, which in the end overthrew the government of Afghanistan, and perhaps most importantly harboured Osama bin Laden. To be sure, it would have been hard at the time to raise cautions about putting pressure on Moscow based on analysis of second-order, and thus iffy, effects.

Likewise, the decision to remove Saddam Hussein was a tactical success but a strategic disaster. It did remove from power a brutal dictator, but the second-order effects created a power vacuum filled by Iran, opened space for the rise of ISIL and intensified the Cold War between Saudi Arabia and an empowered Iran. Nowhere is this failure clearer than five years after the invasion. While visiting Iraq, Iranian President Mahmoud Ahmadinejad was greeted with an elaborate state visit, while a mere two weeks later, Vice President Cheney had to be flown under secrecy (Maloney 2008). America's later decision to leave Iraq left a power

vacuum that enabled the Islamic State to rapidly expand. In short, although tactical intelligence is essential in planning an action, it needs to be viewed in light of more strategic intelligence, intelligence that seeks to parse longer term implications and second-order effects of an action.

Building – and adjusting – “stories” in a shapeless world

The shapelessness of the world both confounds and demands strategic analysis. In providing strategic analysis, I have come to think that intelligence is ultimately about telling stories and most intelligence – or warning – failures derive from holding onto stories that events have outmoded. This challenge is akin to the strategic/tactical challenge facing intelligence and one that bears more directly on warning. A story from another realm, medicine, drives the point home. The medical community had a “story” about the Ebola virus: because death was quick, contagion was unlikely and so the disease would flare up and die out in remote regions. The story was right until it wasn’t: the story had been overtaken by better transit from rural to urban areas. This outdated story led to cases in the United States and to widespread, if not entirely founded, fear of an Ebola pandemic (World Health Organization 2015).

If intelligence is storytelling, many of our current stories are suspiciously long in the tooth. In policy terms, for instance, we have been telling ourselves the same story about North Korea for a generation. With just the right combination of carrots and sticks – primarily the latter – and with China as a real partner, we can induce North Korea to forswear nuclear weapons. Meanwhile, North Korea has gone from an incipient nuclear power to a real one. Intelligence cannot prove and thus cannot say the truth: North Korea is a nuclear power and almost certainly will remain one; that is all the regime has.³ But at the very least, challenging the prevailing story would be a start.

For other critical issues, like the Middle East, we have no real story beyond demonizing terrorists and Iran. To be sure, the task is hard. Throughout my tenure at the NIC, I looked for strategic insights and found precious few because the issues are complicated, and the causal arrows tangled. The best story I found came from our Australian intelligence colleagues. They divided the conflicts into three and a half factions – the ISIL-led Sunni extremists; the Saudi-led Sunni autocrats; the Iran-led Shias and the missing half, the Muslim Brotherhood-led Sunni moderates, recognizing that the term “moderate” is relative at best. But the difficulty of the task is no justification for not trying it. Without a story, we can all too easily blunder into major campaigns against minor threats or worse yet, create those threats.

In the past, America has shown its ability to alter an existing story to great effect. Perhaps most famously, the US decision to recognize the communist China at the expense of Taiwan and treat the country as a counterweight to the Soviet Union was a great success. This partnership fractured the communist world and helped further isolate the Soviet Union. When Nixon and Kissinger decided to covertly meet with Mao, they did this without warning the State Department or

US allies (notably Japan and Taiwan), fearing pushback. Yet once the new story was set, it paved the way for what seemed impossible a few years before – better Sino – American relations (Hutchings and Treverton 2018). Likewise, America’s decision to partner with its old enemy, communist Vietnam, against an ascendant China, shows that reshaping stories can strengthen American policy (Albert 2019).

Transparency and “big data”

These are two sides of the same coin. The same ubiquity of information that produces so much for intelligence agencies to assess also makes it impossible for intelligence operatives to remain secret for long. This, alas, guarantees that there will be more leaks of methods, if not more leakers, like Edward Snowden. Perhaps the vision of the future should be more akin to Silicon Valley, where secrets are kept but not for long and where the premium is on collaboration even if today’s partner may be tomorrow’s competitor.

At the NIC, I was only an observer to intelligence *operations*, but I had the sense that, with respect to clandestine operations, the United States was like the roadrunners in the old cartoons: when they ran off the cliff they didn’t start to fall until they looked down. Given biometrics, facial recognition and ubiquitous cameras, US spy tradecraft has run off the cliff; it just hadn’t looked down yet. Surely, operating under official cover without the knowledge of the host government will become all but impossible. Before I left the RAND Corporation, a retired former CIA station chief joined us. The CIA asked him to do a mission in the country where he had been chief. He said he was happy to do it but only under true name. He knew that any effort to operate under cover would be blown and – to say the least – complicate his future private visits to that country.

But that data will be a godsend for intelligence. Indeed, the analytic challenge is greater for intelligence than for private businesses. Businesses care mostly about learning my preferences and predicting where I will be tomorrow so they can besiege me with personalized ads. By contrast, intelligence is trying to sort out a messy world full of noise and misinformation. Yet Artificial Intelligence (AI) is a natural fit for many intelligence tasks. The Open Source Enterprise, for instance, seeks to read every newspaper in the world, in every language, and monitor every television news broadcast, seeking nuggets of new information or insight (Tucker 2020). AI is a natural fit for it. So, too, it is a natural fit for the National Security Agency (NSA), which uses it not just to sort through the massive amount of signals intelligence it collects, looking for anomalies and potential threats, but also for compliance. NSA does lots of “queries” – that’s NSA-speak for getting access to signals intelligence data on an individual – which requires the paperwork of an audit to decide whether that data can be reported. AI won’t replace human oversight, but it can be used to predict the audit results with pretty high confidence.

At the NIC, I started an experiment with the National Intelligence Officer (NIO) for Africa. Its premise was that while there isn’t a huge amount of intelligence gathered on Africa, there is a lot of data out there. Thus, the goal was an existence theorem: if the NIC, with 100 analysts, could make use of data, then any

place in the Intelligence Community could. Not surprisingly, we found that social media and other available data were pretty good at predicting famine and disease. The next step was to cull “tips” from the data: where should analysts look and what connections should they probe that they hadn’t considered.

The NIC also inherited a nifty bit of crowdsourcing that had been developed by the Intelligence Advanced Research Projects Activity (IARPA), intelligence’s counterpart to DARPA. There were two prediction markets: one classified and comprised of intelligence professionals, and the other unclassified and open. The unclassified one was the creation of Philip Tetlock and it had made two important discoveries. Just as some people are better athletes than others, so too, some people are better predictors. His open market came to feature “super-forecasters”.⁴ Even better, a small amount of training improves prediction. Unsurprisingly, the burden of that training is helping people keep an open mind just a few seconds longer.

I used the internal market as a kind of “red cell” – that is, a person or group charged with being contrarian. Here, I looked for places where the prediction market was contrarian: if the experts thought development x was y percent likely but the market was betting $2y$, what was going on? I didn’t care about the numbers; it was the conversation that mattered.⁵ And I hoped to move the market from fairly short-run predictions, which could be settled soon, to longer, more strategic questions. For them, I hoped we might create way-stations on which to bet and, in the process, perhaps do better at constructing what intelligence calls “indicators”.

Breaking the cycle

It has been often said that the canonical intelligence cycle, from requirements through collection to analysis and dissemination, is often short-circuited. That is true enough – no matter how much intelligence agencies dislike it, policy officials will hanker for the next “raw” spy report or intercept. But as a paradigm the cycle is increasingly unhelpful. In this as in many other ways, what worked tolerably well in the Cold War is dysfunctional now. Then, with one overarching and secretive foe, it made a certain sense to ask, in a linear way, what we needed to know and how we might collect it. Even then analysis had a certain industrial quality about it: a friend who was an NSA Soviet analyst recalls starting the day with a large stack of “her take”, the overnight SIGINT collection relevant to her account.

Moreover, the intelligence cycle simply does not operate as it is described. For instance, it is not guidance from policymakers that sets information requirements, but rather the need to fill gaps in intelligence. Furthermore, the information collectors do not wait for clear requirements before beginning to collect intelligence. If they were to do so, they would not have the intelligence collected when it is needed by policymakers and risk being surprised by sudden events (Hulnick 2006).

Before I returned to the NIC, I had become a fan of “activity-based intelligence”, or ABI.⁶ It was developed in the war zones in Afghanistan and Iraq primarily to unravel terrorist networks and identify bad guys. Identifying Osama bin

Laden's driver was one of its successes. ABI amassed information from many sources around particular locations and then used correlations to develop "patterns of life" that would distinguish potential terrorists from ordinary pious Muslims at prayer. For me, its side benefit was creatively disrupting the canonical cycle. It was "sequence neutral": we might find the answer before we framed the question. Think how often in life that occurs; you don't know you were puzzled about something until you find the answer. And in a world of ubiquitous information, ABI doesn't prize secret sources: if information is useful, it's good; if not, it's not. Finally, perhaps advancing age has made me sceptical of the causation that infuses the canonical cycle. I feel more comfortable with correlation: sure, many of the correlations will be spurious but some will be provocative.

Finding new ways to add value

The traditional model of relations between intelligence and policy, one that is not quite fair to blame entirely on Sherman Kent, is stand-offish lest intelligence be "politicized" by too close an association with policy (Kent 2015). It can be characterized, in caricature, as intelligence throwing elegant analyses over the transom to policy – though no young person these days would have any idea what a "transom" is. Intelligence will be producing those elegant products for as far as the eye can see, but much of the Intelligence Community's stock-in-trade is now available openly as technology continues to evolve. For instance, 30 years ago access to satellite imagery and GPS were only available to US government agencies. Yet today, anyone with a cell phone can access this data and often for free from Google. Although agencies like the National Geospatial-Intelligence Agency (NGA) still have access to imagery with better resolution, the gap of capabilities is only closing.

While these developments might be seen as making much of the Intelligence Community obsolete, they present a great opportunity. The widespread availability of open-source intelligence can be used to complement intelligence, providing a clearer understanding of complex issues. In 2014, for instance, a junior Defense Intelligence Agency (DIA) analyst, browsing Russian social media, was able to determine who shot down Malaysia Airlines Flight 17 (Barnes 2014). As another DIA colleague put it: "Selfies are our best friend".

As in other contexts, the language we use is revealing. Traditionally, intelligence officers thought of their policy counterparts as "customers", which connotes an arms-length, transactional relationship, one in which intelligence provides discrete "products". In my first stint at the NIC, I had one "aha" moment, realizing that while we thought we produced National Intelligence Estimates (NIEs), in fact, our product was National Intelligence Officers (NIOs) – people, not paper. They were in a position to have those elevator conversations with policy counterparts, to give advice informally and not have to be too careful about what was "intelligence" and what was "policy". Similarly, in a study I did of the use of the President's Daily Brief (PDB) by the three administrations before Obama, all of the senior officials who spoke to the issue liked the Brief, but they liked the briefer

better. The briefer offered a way to ask for more, or to take the conversation in a direction especially useful to the policy official (Treverton 2013a).

All possible terms have their negatives, but I think of the recipients of intelligence as “clients”, and liken the intelligence-policy connection to that between me and my financial advisor, a client-service relationship, not a business-customer one: he or she knows things I don’t, but the reverse is also true and it is a relationship between equals. I expect the advisor to ask lots of questions and to get better and better at understanding my interests. He or she is bound by professional code neither to sugar coat the truth nor exaggerate confidence levels. And, in the end, if I don’t feel he or she is adding value, I will go elsewhere.

Intelligence as an argument for policy

This, too, is hardly new. In the past times of divided government, Congress was tempted to, in effect, turn intelligence issues into policy choices by mandating that if intelligence caught Iran exporting x , then y sanctions would be automatic. To be sure, the practice was more than uncomfortable for intelligence, for it meant asking intelligence to put a gun to the heads of its policy counterparts in an administration! More recently, in days of intense partisanship, administrations have been tempted to use intelligence to argue for their policy choices. So it was in the run-up to the 2003 invasion of Iraq. The intelligence assessment that Iraq had weapons of mass destruction made it difficult for Democrats in Congress to oppose the invasion and provided policy cover for supporting it. So, future administrations will be tempted to turn intelligence findings into policy choices: imagine if the Intelligence Community had found what it did not find before the Trump administration scuttled the deal – evidence that Iran was persistently cheating on its obligations under the nuclear deal.

Ironically, when intelligence is used as an argument for policy, it can hamper policy decisions if framed incorrectly. Nowhere is this more evident than in decision to release the key judgements of the classified 2007 National Intelligence Estimate on Iran’s Nuclear Intentions and Capabilities. This estimate stated with high confidence that Iran had its nuclear weapons programme. What it meant by “programme”, as a footnote explained, was weapons design and covert enrichment of weapons-grade uranium. It had not stopped the enrichment of uranium – ostensibly for civil purposes – and the report also noted that Iran was keeping open the option to develop nuclear weapons. Yet when this report was released, the key, albeit false, takeaway was simply that Iran had halted its entire nuclear programme. After this report was released, international momentum for increased sanctions on Iran all but evaporated and the outcome was regarded as a great win in Iran (Treverton 2013b).

Moreover, the obvious desire for policymakers to cherry-pick intelligence that supports their policy is a grave issue. In the lead-up to the Iraq War, most analysis concluded that an Iraq with weapons of mass destruction (WMD) did not present a direct or immediate threat to the United States. Although there was widespread belief that Iraq possessed WMD, there was little concrete evidence

proving so. Despite this, the prevailing mind-set, including of those like me who opposed the war, was that Iraq *must* possess WMD, though not nuclear weapons. In that climate, it was difficult for any analysts to make the argument that Iraq had no WMD of any kind, and too easy for policymakers to accept information supporting their beliefs, including from discredited sources like Curve Ball (Heazle 2010).

New competitors, new colleagues

Intelligence has always worried about the competition. A generation ago, the competition was CNN: was intelligence always to be scooped by CNN? (I always thought that concern was misplaced: better to get it right than get it wrong, first). Now, though, the list of sophisticated private organizations doing “intelligence” is a long one, from Eurasia Group through Bloomberg and Oxford Analytica to Stratford.

The Russian intervention in the 2016 US elections came as a surprise, but it should not have. There was warning but from an unfamiliar quarter. A group of analysts outside government was tracking the online dimensions of the jihadists and the Syrian civil war when they came upon interesting anomalies as early as 2014. When experts criticized the Assad regime online, they were immediately attacked by armies of trolls on Facebook and Twitter. Unrolling the network of the trolls revealed they were a new version of “honeypots”, presenting themselves as attractive young women eager to discuss issues with Americans, especially those involved in national security. The analysts made the connection to Russia but found it impossible, that early, to get anyone in the American government to pay attention, given the crises competing for both policy and intelligence attention (Weisburd, Watts, and Berger 2016).

The cyber arena is also a striking example of the change. In the traditional process, if a major hack occurred, it would fall to the Intelligence Community to attribute it to the perpetrator. Afterwards, policy would decide on a response, name and shame, seek indictments or whatever. Now, however, that tidy process is disrupted, for while intelligence is doing attribution, so too are a host of private companies. And they will not be shy about identifying the perpetrator, never mind what the government might prefer. In the short run, this seems competition; in the long run, I hope it will become creative collaboration.

One of the Intelligence Community’s greatest challenges is ensuring it remains useful to policy makers, when they show a marked interest in other sources.

Dealing with the Trump train wreck, especially truth as malleable

So much for the future of intelligence in normal times. Like many Americans, I thought the pressure of governing would compel Mr. Trump to behave like a more usual president, despite the deep distrust in the bureaucracy of the Intelligence Community he had expressed during the campaign. But he did not; he was more prone to turn to Fox News than the Intelligence Community for advice.

The most visible damage, one which the new Director of National Intelligence (DNI), Avril Haines, emphasized in her confirmation hearings, was to the morale of the workforce, especially that of the Office of the DNI.⁷ It is one thing to suffer the privations of money and lifestyle to serve as an intelligence officer if you feel your work is valuable and recognized as such. Who would do it, though, if your work was dissed and you were at risk of being thrown under the bus for any deviation from the party line in a blatantly politicized ODNI? The three-letter agencies, CIA and its kin, were mostly, though not entirely, shielded from the political manipulations, so the damage is less there. For the ODNI, the simple fact of working for a president who values intelligence and a director who doesn't dismiss or twist it should restore morale fairly quickly. The longer term cost in the coin of those who left or shunned intelligence service is harder to reckon.

The January 6, 2021 riots at the Capitol underscored the need to reshape domestic intelligence, a need reflected in the president's charge to the director later in the month to produce a thorough assessment of domestic terrorism. White supremacist groups were responsible for 41 or 61 terrorist incidents in the first eight months of 2020.⁸ Yet the nation's sprawling counterterrorism apparatus, while adapting, remains preoccupied with Islamic terrorism, not to mention the former president's continual conjurings, virtually all baseless, of "antifa terrorism" on the left.

More broadly, domestic intelligence continues to be something of a stepchild in the US Intelligence Community, which is dominated by agencies, like CIA and NSA, whose mandate and mindset are limited to "foreign" intelligence. The raggedy connections among the "domestic" agencies, especially FBI and DHS, and between them and state and local law enforcement were, sadly, all too apparent on January 6.

The last challenge is existential, for intelligence now faces a world not just of "false" facts and presidential tweets of bald disinformation, and the prospect that "truth" will be widely regarded as personal, or political, or partisan, but also one in which the very concept of truth – that empirical realities can validate or invalidate spoken statements – is under assault. One of the great paradoxes of our times is that all the wonderful technology created to connect people has ended up segmenting them into "echo chambers" in which they hear only what they want and learn only what they already thought.

In passing, while I came to admire the marble entrance hall at the CIA, I've always found the Biblical quotation from John – "ye shall know the truth, and the truth shall set you free" – odd, and oddly placed there. Intelligence, still more than other endeavours, has always known how elusive the truth can be. And our language, like "true enough", is mirrored in the distinction between intelligence and law enforcement: true enough for policy is a looser standard than true enough for a court of law. And in effect, and sometimes in intent, intelligence's truth is more likely to constrain policy than to "set it free".

So far, I see no better response for intelligence than to double down on trying to distinguish what is likely true from what is not. False facts, in principle, make real ones more valuable and their identification more pressing. Haines put

it well: “The greatest challenge . . . is building the trust and confidence necessary to protect the American people. To be effective, the DNI must never shy away from speaking truth to power – even, especially, when doing so may be inconvenient or difficult. To safeguard the integrity of our Intelligence Community, the DNI must insist that, when it comes to intelligence, there is simply no place for politics – ever.”⁹

The question is: will anyone listen? I fervently hope so.

Notes

- 1 I thank Stephen Chesterman for valuable research and comment in the final preparation of this article.
- 2 For an assessment of what it would take for the United States to both think and act more strategically, and for examples of when the country has, see Hutchings and Trevorton (2018).
- 3 The only country to develop its own nuclear arsenal, and later denuclearize is South Africa in 1989. At that time the apartheid was coming to an end and South Africa was working on ending its pariah status in the International Community. There are no clear parallels between the democratizing South Africa and ever authoritarian North Korea (Friedman 2017).
- 4 For more on this topic see Tetlock and Gardner (2015).
- 5 On red-teaming, see Zenko (2015).
- 6 For a thorough introduction to ABI, see Biltgen and Ryan (2015).
- 7 The hearings, including her statement, are available at www.intelligence.senate.gov/hearings/open-hearing-nomination-avril-haines-be-director-national-intelligence.
- 8 CSIS Issue Brief, *The War Comes Home: The Evolution of Domestic Terrorism in the United States*, October 22, 2020, available at www.csis.org/analysis/war-comes-home-evolution-domestic-terrorism-united-states.
- 9 Haines, cited earlier.

References

- Albert, Eleanor. 2019. “The Evolution of U.S.-Vietnam Ties”. *Council on Foreign Relations*, March 20. www.cfr.org/backgrounder/evolution-us-vietnam-ties.
- Barnes, Julian E. 2014. “U.S. Military Plugs into Social Media for Intelligence Gathering”. *Wall Street Journal*, August 6, sec. US. <https://online.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557>.
- Biltgen, Patrick, and Stephen Ryan. 2015. *Activity-Based Intelligence: Principles and Applications*. Boston: Artech House.
- Friedman, Uri. 2017. “There Is No Precedent for What America Wants from North Korea”. *The Atlantic*, September 6, sec. Global. www.theatlantic.com/international/archive/2017/09/history-north-korea/538800/.
- Heazle, Michael. 2010. “Policy Lessons from Iraq on Managing Uncertainty in Intelligence Assessment: Why the Strategic/Tactical Distinction Matters”. *Intelligence and National Security* 25 (3): 290–308. <https://doi.org/10.1080/02684527.2010.489780>.
- Hulnick, Arthur S. 2006. “What’s Wrong with the Intelligence Cycle”. *Intelligence and National Security* 21 (6): 959–79. <https://doi.org/10.1080/02684520601046291>.
- Hutchings, Robert L, and Gergory F. Trevorton. 2018. *Rebuilding Strategic Thinking*. Washington, DC: CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181018_RebuildingStrategicThinking_WEB_v2.pdf.

- Kent, Sherman. 2015. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press.
- Malley, Robert, and Jon Finer. 2018. "The Long Shadow of 9/11". December 7. www.foreignaffairs.com/articles/2018-06-14/long-shadow-911.
- Maloney, Suzanne. 2008. "How the Iraq War Has Empowered Iran". *Brookings* (blog). March 21. www.brookings.edu/opinions/how-the-iraq-war-has-empowered-iran/.
- Tetlock, Philip E., and Dan Gardner. 2015. *Superforecasting: The Art and Science of Prediction*. New York: Crown.
- Treverton, Gregory F. 2013a. *First Callers: The President's Daily Brief across Three Administrations*. Washington, DC: Center for the Study of Intelligence; Central Intelligence Agency. www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/csi-intelligence-and-policy-monographs/pdfs/first-callers.pdf.
- . 2013b. *Support to Policymakers: The 2007 NIE on Iran's Nuclear Intentions and Capabilities*. Washington, DC: Center for the Study of Intelligence; Central Intelligence Agency. www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/csi-intelligence-and-policy-monographs/pdfs/support-to-policymakers-2007-nie.pdf.
- Tucker, Patrick. 2020. "Spies Like AI: The Future of Artificial Intelligence for the US Intelligence Community". *Defense One* (blog). January 27. www.defenseone.com/technology/2020/01/spies-ai-future-artificial-intelligence-us-intelligence-community/162673/.
- Weisburd, Andrew, Clint Watts, and J. M. Berger. 2016. "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy". *War on the Rocks* (blog). November 6. <https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/>.
- World Health Organization. 2015. "Factors That Contributed to Undetected Spread". January 2015. Accessed December 17, 2020. www.who.int/news-room/spotlight/one-year-into-the-ebola-epidemic/factors-that-contributed-to-undetected-spread-of-the-ebola-virus-and-impeded-rapid-containment.
- Zenko, Micah. 2015. *Red Team: How to Succeed By Thinking Like the Enemy*. 1st edition. New York: Basic Books.