Adam I. Klein

The Cyclical Politics of Counterterrorism

On a summer night in late August 2001, the United States launched a massive surprise assault on al-Qaeda and Taliban targets in Afghanistan. Moments after the bombs and cruise missiles stopped falling, elite special-forces commandos landed at Osama bin Laden's Tarnak Farms camp, killing bin Laden and dozens of his lieutenants. As the commandos' helicopters took off from the devastated camp, they carried a massive haul of valuable intelligence—al-Qaeda records, hard drives, and cell phones used by the terrorists.

Analysts at the CIA's Counterterrorist Center (CTC) immediately tore into this trove, hunting for any clues about potential al-Qaeda attacks on the U.S. homeland. They had good reason to fear such plots. Intelligence reporting that summer had produced a steady "drumbeat" of warnings that bin Laden was planning an attack in the United States or on our close allies. In the words of Director of Central Intelligence George Tenet, "the system was blinking red." The President's Daily Brief (PDB) given to President George W. Bush on August 6, 2001, had included an article titled "Bin Ladin Determined to Strike in US," the "36th PDB item briefed so far that year related to Bin Ladin or al-Qaeda."[1]

What CTC's analysts discovered exceeded even the worst fears of those who had urged the assault on bin Laden: al-Qaeda had planted sleeper operatives in the United States and planned to conduct a spectacular wave of simultaneous hijackings. By cross-referencing names found in the materials recovered from the camp with State Department and Immigration and Naturalization Service (INS) records, the FBI was able to identify and arrest several Saudi and Yemeni al-Qaeda operatives who had infiltrated the United States. Under interrogation,

Adam Klein is a Senior Fellow at the Center for a New American Security, where he studies counterterrorism, surveillance policy, and national security law. He can be reached at aklein@cnas.org.

The Washington Quarterly • 40:2 pp. 95–111
https://doi.org/10.1080/0163660X.2017.1328926

one of them revealed that they planned to hijack airliners using box cutters and then fly the planes into prominent buildings. While the FBI rolled up the remaining sleeper agents, the Federal Aviation Administration (FAA) mandated stringent aviation security measures to prevent suicide hijackings. And the 'Summer of Threat' gradually faded into a quiet autumn.

This is a fantasy, of course. We did not invade Afghanistan in the summer of 2001. Tragically, we did not uncover al-Qaeda's plans. We were not able to stop the 9/11 attacks. Yet none of the steps in this imagined chain of detection and disruption is farfetched. Even the military assault had been contemplated: a draft presidential directive circulated in June 2001 instructed Secretary of Defense Donald Rumsfeld to "'develop contingency plans' to attack both al-Qaeda and Taliban targets in Afghanistan."[2] The national security bureaucracy was aware of the threat from al-Qaeda and its desire to carry out mass casualty attacks in the United States, and had a general sense of the level of effort that would be needed to neutralize the threat.

The problem is that the American people almost certainly would not have supported a unilateral preventative war against al-Qaeda and the Taliban that summer. President Bush told the 9/11 Commission that the draft presidential directive signaled his "readiness to invade Afghanistan," and that he had been willing to "take on" the inevitable political repercussions. Yet he acknowledged that "the problem would have been how to do that if there had not been another attack on America. To many people … it would have seemed like an ultimate act of unilateralism."[3]

The urgent, improvisational post-9/11 climate yielded excesses many Americans now regret.

It is impossible to test President Bush's counterfactual, but it rings true. To the American people, this was peacetime. The key policy debates that summer were the No Child Left Behind education reform bill and the Bush administration's disavowal of the Kyoto Protocol climate treaty. It is hard to imagine that the public would have welcomed a large-scale military strike against a terrorist group most Americans had never heard of, and whose deadliest attacks on U.S. interests had taken place in countries (Tanzania, Kenya, Yemen) most Americans knew little about.

All of that changed on September 12. Leaders who two days before lacked the political capital to strike al-Qaeda now found themselves scrambling to satisfy the public's demand for vengeance and to assuage fears of further attacks. Over the next few years, that momentum drove massive reforms in the national security

bureaucracy, coupled with an all-out effort to destroy al-Qaeda and secure the homeland. Those furious efforts largely succeeded—we have not had another attack on the scale of 9/11. But the urgent, improvisational climate also yielded some excesses that many Americans now regret.

The post-9/11 cycle—an unexpected crisis, a hasty reaction, and then a gradual reconsideration and dialing back of the strong measures initially taken—is anything but an outlier. Rather, it is emblematic of the political dynamics that shape counterterrorism policymaking in our democratic system.

"Crisis Lawmaking"

Of course, it is hardly a new insight that historic policy reforms often emerge from crises. (Or, to put it more cynically, that crises provide a window of opportunity for policymakers to push through long-desired changes.) Nor is this dynamic limited to national security crises. During the 2008 financial crisis, Obama's first chief of staff Rahm Emanuel, borrowing an aphorism attributed to Winston Churchill, famously told reporters that "[y]ou never want a serious crisis to go to waste."[4] The import, of course, was that the crisis gave the administration a political window to achieve long-sought elements of the Democratic Party's domestic agenda. The 2009 stimulus bill and the 2010 passage of the Affordable Care Act proved him right.

Crises are a rare opportunity for legislative boldness because policymaking in a democratic system follows public opinion. In our vetogate-rich legislative process, public opinion ordinarily constrains action, as a balance of "opposite and rival interests"[5] prevents any side from achieving its ideal end. In times of crisis, however, public opinion swings dramatically to one side and not only permits but *compels* action in that direction. Those deft enough to harness the public's clamor for a swift response can effect changes that would be unachievable under ordinary political conditions. The cynical account of this dynamic is that devious politicians exploit crises to ram through their partisan agendas. The more charitable version is that crises concentrate the public's attention on an issue, empowering public-spirited reformers to overwhelm the entrenched special interests that ordinarily protect the status quo. Whether an observer views a given act of crisis lawmaking as legitimate likely depends more on his or her view of its merits as policy rather than a neutral theory of the legislative process.

> Public opinion about counterterrorism differs in fundamental ways from domestic policy issues.

Importantly, however, public opinion about counterterrorism—and thus the role of crisis lawmaking in setting counterterrorism policy—differs in fundamental ways from public opinion about health care, taxation, education, or other domestic policy issues. Because it is largely secret, and because much of it takes place overseas, counterterrorism is, ordinarily, remote from the average American's daily existence. Only an attack on the homeland or some exceptionally horrific act overseas captures the attention of the average person. Indeed, even exceptionally horrific attacks overseas often fail to penetrate the American public's consciousness. How many Americans recall the horrific attack on Kenya's Garissa University, where just two years ago al-Shabaab massacred 147 students, singling out Christians for cold-blooded execution? Or the October 2015 bombing of Metrojet Flight 9268 from Sharm el-Sheikh, Egypt, to St. Petersburg, perpetrated by ISIS's Sinai affiliate, which killed 224 Russian tourists and crew?

Domestic policy, by contrast, constantly intrudes into our day-to-day existence. Voters are reminded of health policy every time they search for a new insurance plan or get a bill from a health-care provider. They see the effects of tax policy with each pay statement, and education policy at every parent-teacher conference. There are few elections where taxation, health care, and education are not prominent themes. Terrorism, by contrast, becomes a leading issue only when some searing event forces it onto the political agenda.

Another significant difference is that on many major domestic policy issues, change is evolutionary rather than sudden. Crime ticks up, class sizes slowly expand, wages and the cost of living gradually climb or decline. Pressure for reform builds slowly, giving interest groups and policy experts years to develop and debate possible responses. Terrorism, however, is inherently sporadic—quiet periods suddenly shattered by extreme violence. The result is that public opinion on counterterrorism does not ebb and flow; it lurches from one extreme to the other.

The effect of this volatility, coupled with Congress's inability to regularly reopen controversial legislation, is that counterterrorism policy is uniquely shaped by crisis lawmaking. This is powerfully illustrated by the fact that legislation passed in the immediate wake of 9/11 continues to govern much of our counterterrorism response. For example, the Authorization for the Use of Military Force (AUMF) against those responsible for the 9/11 attacks—a bill passed on September 18, 2001—remains, fifteen years later, the principal legal basis for the United States' ongoing use of military force against terrorist groups. That bill authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines *planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001*, or harbored such organizations or persons" [emphasis added].[6] Put simply, the law authorized

military force against those entities involved in the 9/11 attacks, or those who harbored them.

In the intervening fifteen years, however, its use has expanded far beyond the groups and countries Congress contemplated in 2001. The executive branch has relied on the AUMF to target, among others, al-Shabaab, which did not exist in 2001, and ISIS, which not only did not exist in 2001 but has since openly broken with al-Qaeda. (As to al-Shabaab, the rationale is that it is an "associated force" of al-Qaeda. As to ISIS, the rationale is that it shares al-Qaeda's DNA because it grew out of al-Qaeda in Iraq, which pledged fealty to Osama bin Laden in 2004.) Remarkably, the full of list of groups the United States considers covered by the 2001 AUMF remains classified—a fitting metaphor for the sixteen-year shadow war against global jihadism.[7] Geographically, our conventional military operations against jihadist networks have spread from Afghanistan—the foreseeable locus of military operations when Congress authorized them in 2001—to at least six countries, most recently Syria. And that excludes countries (most notably, Pakistan) where the U.S. government has launched covert paramilitary operations against jihadist groups, as well as the long list of countries where U.S. forces have been deployed to train, advise, and assist local counterparts in their own counterterrorism missions.[8] All this has happened without Congress once updating, or even reaffirming, the authorization.

None of this is to say that it is wrong to apply the 2001 AUMF to al-Shabaab or ISIS, or to read it as authorizing operations outside Afghanistan. To the contrary: there are strong legal arguments for each of these positions.[9] Yet, it is nonetheless remarkable that a 60-word paragraph, enacted in the chaotic aftermath of a catastrophic attack, continues to set the parameters of a 15-year-old, globe-spanning conflict.

Another illustration is the USA PATRIOT Act, which President Bush signed into law on October 26, 2001. One provision of the Act, Section 215, became famous in 2013 when the Edward Snowden leaks revealed how the government was using it. Section 215 authorized the FBI to request a court order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism" or foreign espionage if it could show reasonable grounds to believe that the records sought were "relevant to an authorized investigation."[10] The Snowden leaks disclosed that the government had obtained a court order under this provision allowing the NSA to collect *all* telephone call records generated by major U.S. carriers, including records of calls made by ordinary, law-abiding Americans. This program continued until 2015, when it was substantially curtailed by the USA FREEDOM Act.[11] The long and unexpected life of Section 215 illustrates how legislation hastily enacted in the aftermath of terrorist attacks can

shape counterterrorism responses for years to come, in ways that are hard to foresee at the outset.

Perception and Reality

A key feature of counterterrorism politics is that the public's *perceived* level of threat, not the *actual* level of threat, determines the public demand for security measures—and there is typically a significant difference between the two. Why? The public typically underestimates the terrorist threat during periods of quiet, for several reasons. One is that counterterrorism officials often keep foiled attacks secret in order to preserve the intelligence sources and methods that enabled them to detect the plot. For example, the Obama administration was rightfully infuriated by media reports detailing how al-Qaeda in the Arabian Peninsula (AQAP) handed a state-of-the-art, second-generation underwear bomb to a mole run by Saudi intelligence.[12] Keeping successes out of the news helps prevent terrorist groups from discovering the means used to accomplish them. A lamentable but unavoidable consequence of such discretion is that the public is not fully apprised of the scale, sophistication, and ambition of the country's terrorist enemies.

Even when failed or disrupted plots become public, however, the public tends to ignore or undervalue these near-misses. How many Americans remember the underwear bomb that almost brought down Northwest Airlines Flight 253 on Christmas Day 2009, which would have killed 259 people? How many remember the Millennium Plot, when al-Qaeda sleeper agent Ahmed Ressam tried to enter the United States with a hoard of bomb-making materials and plans to bomb Los Angeles International Airport on December 31, 1999? How many Americans even noted these events when they happened? Arguably, these near misses were as strong an indication of al-Qaeda's capabilities and intentions as they would have been if they had succeeded. Yet, they did not precipitate counterterrorism legislation proportional to the threat they revealed.

In fact, even *successful* al-Qaeda attacks on U.S. interests overseas did not sufficiently shift public opinion in the years before 9/11. Al-Qaeda bombed two U.S. embassies in East Africa in 1998 and the U.S.S. *Cole* in Yemen in 2000. Those attacks were widely reported, yet terrorism did not become a politically salient issue until after the 9/11 attacks. The 9/11 Commission noted that "neither in 2000 nor in the first eight months of 2001 did any polling organization in the United States think the subject of terrorism sufficiently on the minds of the public to warrant asking a question about it in a major national survey." Terrorism "was not an important topic in the 2000 presidential campaign," and "Congress and the media called little attention to it."[13] These pre-9/11 attacks left no doubt that bin Laden's threats against the United States were meant in earnest

and backed by substantial capability, but they happened in faraway places and did not register in the public consciousness. Unfortunately, the public was roused to demand strong counterterrorism measures only after al-Qaeda struck the homeland.

If foiled attacks and attacks overseas do relatively little to alert the public, subtler warning signs have even less of an effect. Osama bin Laden's pre-9/11 fulminations and fatwa against the United States, though widely reported, barely dented the public consciousness. More recently, ISIS's rise in late 2013 and early 2014 had been heavily covered and analyzed in the media for months before its gruesome beheading videos awakened most Americans to the danger it posed. In late June 2014, less than two weeks after ISIS forces conquered Iraq's second-largest city, Mosul, a CBS News/*New York Times* poll reported that only 29 percent of Americans supported doing more to address the violence in Iraq; 51 percent opposed using piloted aircraft (as opposed to drones) to support Iraqi forces; 77 percent opposed ground troops; and 57 percent said that the situation in Iraq is "beyond the control of the United States."[14] Just two months later, the death of one person—the American journalist James Foley, whom ISIS brutally beheaded on camera in the Syrian desert—reversed the situation completely. Now, 71 percent favored airstrikes against ISIS terrorists in Iraq; 69 percent favored airstrikes against ISIS in Syria; 39 percent even supported sending ground troops into Iraq or Syria.[15] ISIS's breathtaking territorial conquests, a geopolitical earthquake with massive significance for the region and the world, barely dented the public consciousness. It took the horror of Foley's death—which, while a shocking affront to the conscience of the civilized world, was not necessarily a reliable signal of ISIS's level of capability or broader threat to the West—to rouse the American people to action.

Foiled attacks and attacks overseas do relatively little to alert the public.

A final factor is that classified intelligence reports and analysis, which can provide early warning of emerging terrorist threats, are by their nature invisible to the public and the press. Intelligence reports showing that terrorists are developing new and dangerous capabilities should and do spur policymakers to take measures to preempt the threat. For example, the United States and United Kingdom recently banned laptops and tablets on flights from certain Middle Eastern countries because intelligence suggested that AQAP was "perfecting techniques for hiding explosives in batteries and battery compartments of electronic devices."[16] But unless classified intelligence reporting is declassified (which is often precluded by the need to protect intelligence sources and methods) or leaked (which raises the same sources-and-methods concerns, and is illegal) it does not generate public support for measures that are a heavy political lift. It is

hard to imagine, for example, that the American public would have accepted the recent laptop ban had it applied to all domestic flights, or even to international flights from common vacation destinations like Mexico, the Caribbean, or Western Europe.

Short of actual, successful attacks on the U.S. homeland, signals of threat that concern terrorism experts—foiled attacks, attacks overseas, declarations of intent to attack the United States, rising ideological extremism, classified intelligence reporting—do not significantly move the public's perception. This means that the public is likely to underestimate the true danger posed by a group that has not yet struck the homeland or otherwise succeeded in penetrating the public's consciousness.

By contrast, counterterrorism professionals and others who work in the space (journalists, academics, etc.) closely track these subtler indicators of a growing threat, and thus are likely to have a far more accurate threat perception. These observers are also far better informed about the geopolitical, economic, and intellectual currents which influence the threat's expansion or remission. It follows that during periods of ostensible calm, counterterrorism professionals are likely to perceive terrorist threats where the general public does not. After the 1998 embassy bombings, CIA Director George Tenet told senior Agency officials: "We are at war. I want no resources or people spared in this effort … "[17] The public, unfortunately, did not perceive the United States to be at war with al-Qaeda until September 12, 2001. The result was that counterterrorism professionals who were aware of the gravity of the threat and sought a more aggressive policy against al-Qaeda—such as a CIA presence in Afghanistan and missions to kill or capture Osama bin Laden—lacked the political capital to win approval of those measures until after the 9/11 attacks.[18]

On the other extreme are *successful* attacks on the homeland, which have an immense and arguably disproportionate effect on the public's threat perception. As former 9/11 Commission staff member William Johnstone has noted, those attacks moved the public "from an under-appreciation of the terrorist threat to a wildly exaggerated overestimate of what was, in essence, the same threat that had existed for some time."[19] This reflects a cognitive bias known as the availability heuristic: the tendency to assess as more probable prominent events that can be easily recalled.

A corollary here is that particularly gruesome events, like the videotaped beheadings for which ISIS is notorious, can rivet the public's attention—and drive political action—regardless of whether they are indicative of a broader threat to the homeland. There are various psychological and cultural explanations for why beheadings "produce an extraordinarily potent artefact that compels our attention[,] whether we like it or not," explains anthropologist Frances Larson.[20] Yet whatever the reason, the ISIS beheadings galvanized the American

public in a way that ISIS's military successes and innumerable prior atrocities had not. The broader point is that the public's threat perception overlooks many events that are sound indicators of a brewing threat, while spiking disproportionately in response to others.

Counterterrorism experts perceive the threat more accurately, but lack political capital.

Putting all of this together yields three key takeaways. First, during high-threat quiet periods, counterterrorism professionals and experts will perceive the threat more accurately than the public, but will frequently lack the political capital to obtain their preferred policies. The 9/11 Commission's Executive Director, historian Philip Zelikow, has spoken of the "paradox of prevention": the political difficulty of taking "massive action" to counter a potential threat before its scale is apparent to the public.[21]

Second, while the public demand for counterterrorism may be unduly low in periods of ostensible quiet, it spikes in the aftermath of a major attack. A useful metaphor is the economic concept of "elasticity": the degree to which demand for a given product varies depending on its price. Public demand for counterterrorism measures is highly elastic—it moves wildly in response to recent, successful, emotionally salient (and, relatedly, *visually* captivating) terrorist acts. By contrast, demand for ordinarily public goods—health care, education, infrastructure—is relatively inelastic; it does not fluctuate to the same extent with the vicissitudes of the news cycle.

An important corollary here is that the public's demand for counterterrorism measures is *more elastic than it should be*. That is because the public is generally unaware of evidence of a latent or growing threat, meaning that during periods of relative quiet, its threat perception is unduly low. But once the threat manifests itself in a successful, politically salient attack, the public's threat perception, and thus its demand for counterterrorism measures, skyrockets. This volatility, while explicable, is nonetheless irrational: the threat was present, and was likely discerned by experts, all along.

Third, this pattern—insufficient action during quiet periods followed by post-attack overcorrections—obviously impedes counterterrorism, but it is also detrimental to civil liberties. Nothing is worse for civil liberties than a successful attack, because major attacks compel an immediate, strong response that reassures a fearful public. And in the post-attack political climate, civil libertarians' ability to influence counterterrorism legislation is at its lowest ebb. The PATRIOT Act, for years afterwards a *bête noire* of civil libertarians, passed with only one "no" vote in the Senate and only 66 in the House. In the wake of the horrific November 2015 terrorist attacks in Paris, the French government decreed a state of emergency permitting police to conduct extrajudicial warrantless searches of homes

and businesses. In December 2016, France's National Assembly reauthorized the state of emergency by an overwhelming majority—unsurprising given that more than 80 percent of the French public supports either preserving or expanding it.[22] What percentage of the French public would have supported warrantless searches and police-imposed movement restrictions had the Paris attacks been foiled?

The bind for civil libertarians is that preventive security measures, which may be in tension with customary American attitudes toward privacy and law enforcement, may avert attacks and thus prevent reactive measures that are far more expansive. The Obama administration recognized that the attempted underwear bombing on Christmas Day 2009, had it succeeded, would have utterly changed the political outlook for the president's first term. That realization reportedly jolted the administration into a much more aggressive posture on counterterrorism, especially against AQAP, which was behind the attempted bombing.[23] One result was the 2011 drone strike that killed Anwar al-Awlaki, the American imam turned terrorist preacher who inspired the 2009 Fort Hood shooter, the underwear bomber, and (posthumously, through his recorded sermons) the brothers who bombed the 2013 Boston Marathon.

Civil-liberties groups naturally object to targeted killings; in 2010, after media reports suggested that Awlaki's name appeared on internal government "kill lists," the ACLU and Center for Constitutional Rights helped Awlaki's father file a lawsuit seeking to bar the government from killing him.[24] (The lawsuit was dismissed on procedural grounds.) Yet, how many potential Fort Hoods and Boston Marathons did Awlaki's killing prevent? And what security measures would those attacks have triggered?

Resisting the Cycle

The cyclical politics of counterterrorism are intuitive, but difficult to resist. Ideally, during quiet periods, policymakers and civil liberties groups would have a shared interest in implementing those reasonable measures that would swiftly pass in the aftermath of the next attack—reducing the risk of both an attack and, therefore, the more aggressive measures that would follow one. In practice, civil liberties groups will rarely make concessions unless their ideologically committed members—who expect zealous advocacy, not collaboration with those in power—see those concessions as absolutely unavoidable. Of course, that realization tends to set in only after a major attack. At

The cyclical politics of counterterrorism are intuitive, but difficult to resist.

that point, hawks, flush with political capital, no longer need to compromise.

Meanwhile, most members of Congress are unlikely to invest significant political capital in counterterrorism unless there has been a major attack or some other searing event that captures the public's imagination. Counterterrorism and homeland security produce votes only when the public *perceives* the threat as high—which, as we have seen, will not happen as long as the threat remains latent. Absent the political imperative spawned by a successful attack, other issues will naturally attract greater congressional attention. As the 9/11 Commission observed in explaining why terrorism was not a higher priority in the 1990s, "Congress always has a strong orientation toward domestic affairs"; indeed, even "Presidents are selective in their use of political capital for international issues."[25] And intelligence and counterterrorism, unlike big-ticket defense acquisition programs or military bases, do not generate visible economic returns for home districts. The result is that that members of committees responsible for intelligence, counterterrorism, and homeland security, who are briefed on and tend to be most motivated to confront latent or emerging threats, may struggle to persuade their colleagues of the need for proactive measures to counter those threats. Meanwhile, with civil liberties groups prepared to resist new security measures, boosting counterterrorism during a quiet period requires Congress and the president to expend significant political capital. There are no easy lifts—except during a post-attack crisis.

Current policy stalemates illustrate the difficulty of finding reasonable security-enhancing compromises to address looming threats without the impetus of a mass-casualty event. For instance, it has been widely reported that ISIS instructs its recruits to use end-to-end encryption (that is, encryption that permits only the end-users to view decoded messages). Yet, the FBI has struggled to make headway in its quest for means to circumvent or otherwise cope with such encryption. Indeed, an Obama-era National Security Council review of potential approaches to the encryption issue did not even include seeking legislation among the options considered. (The three options considered were explicitly disavowing legislation; publicly declining to seek legislation for the time being; or simply saying nothing.)[26]

There are, of course, legitimate arguments against legislation limiting end-to-end encryption. Requiring companies to build in a government-access mechanism, or even to maintain their own ability to decrypt data stored on their products or platforms, "would introduce a certain (albeit unquantified) degree of additional insecurity into those products."[27] Some also argue that a U.S. decryption mandate would induce authoritarian regimes to seek equivalent access, although this argument likely overstates U.S. influence and underestimates authoritarian adversaries' determination to access desired data regardless of what the United States does.[28] Finally, forcing private citizens to store their personal data in a

manner designed to facilitate government surveillance would have been intolerable to the founding generation and would sit awkwardly within our traditions of individual liberty and privacy. Yet these arguments, however meritorious, would likely have little purchase in the aftermath of a mass casualty attack on the U.S. homeland, if the attackers turn out to have exploited end-to-end encryption.

Events overseas suggest as much. Police raids following the 2015 Paris attacks recovered at least one encrypted iPhone that French investigators have been unable to open. In response, France's National Assembly adopted an amendment authorizing a €350,000 fine for companies and *five years' imprisonment* for corporate executives who refuse, in a terrorism investigation, to break encryption their companies created. That proposal did not become law, but it illustrates the type of measures that might follow a mass casualty attack. The adversarial stalemate over encryption in the United States makes it more likely that a future attack will yield hastily devised legislation whose features are uncongenial for end-to-end encryption's defenders today.

The quest to improve the nation's cybersecurity is another useful illustration. A steady succession of damaging cyberattacks, intrusions, and data breaches has made cybersecurity an urgent priority. Chinese hackers reportedly stole plans to the United States' cutting-edge F-35 fighter and swiped millions of security clearance records from the Office of Personnel Management, a counterintelligence disaster. Cybercriminals have stolen the credit card data of tens of millions of customers at Home Depot, Target, and other retailers. Unfortunately, despite these lapses, the wider public is not yet deeply engaged in the urgent challenge of securing the nation's networks, even after the consequential Russian hacks of Democratic Party institutions and individuals in 2016. Lacking the political capital generated by a catastrophic event, Congress has struggled to pass even relatively modest, bipartisan cybersecurity legislation.[29] Yet, does anyone doubt that significant legislation would pass swiftly if a massive cyberattack were to trigger a panic in the financial system, release a devastating flood by remotely opening a dam, or disable large swathes of the electric grid?

There are no easy fixes for these dynamics, which stem from deep-seated psychological tendencies and fundamental political realities. Human beings estimate future risk based on recent past events—especially those that are particularly gruesome and terrifying. And in a democratic system, politicians are usually constrained to follow the vicissitudes of public opinion rather than anticipating and preempting them. In short, there is probably little that can be done to fundamentally alter the cyclical politics of counterterrorism.

Nonetheless, there are ways to anticipate and to some degree mitigate their effects. One is to educate voters about latent threats before they manifest themselves catastrophically. The former members of the 9/11 Commission have

warned against "counterterrorism fatigue and waning urgency," calling for continued vigilance.[30] Current and former national security leaders, to their credit, have tried furiously to alert Americans to the threat of cyberespionage and cyberattack, using events like high-profile data breaches to hammer home the point. Of course, it is an uphill battle to persuade the public at large to take seriously a dormant or latent threat. But such efforts, if taken up by the media and civil society, can create momentum for security improvements. And any shift in public opinion that eases the political path for reforms, however slightly, marginally reduces the odds of the threat manifesting itself in a catastrophic attack, with all of the human and societal consequences those entail.

A second way to reduce the risk of ill-advised post-attack legislation is to consider in advance what measures would be wise and desirable *if the political capital existed to enact them*. Those responding to a crisis should have a well thought out, pre-vetted set of policy options "on the shelf" in advance of a major crisis. Once the political capital exists, those in a position to act will naturally draw on the work that has already been done. For example, the 9/11 Commission's proposal for a Director of National Intelligence (DNI) drew on earlier proposals dating back at least to 1971, and arguably to 1955.[31] Those decades of study eventually bore fruit when the political climate shifted after 9/11.

There are ways to anticipate and somewhat mitigate the effects of counterterrorism's cyclical politics.

Analogous ground-laying work is being done today. Though Congress has struggled to update the 2001 Authorization for the Use of Military Force, the Obama administration, Members of Congress, and outside observers have produced thoughtful proposals for how Congress might revise the AUMF to account for intervening developments, including ISIS.[32] Similarly, while the encryption debate appears intractable given recent political dynamics, in mid-2016 Senators Richard Burr (R-NC) and Diane Feinstein (D-CA), Chair and former Vice Chair of the Senate Select Committee on Intelligence, drafted legislation requiring companies to either retain the capacity to decrypt data or provide technical assistance to the government as it attempts to do so.[33]

The encryption example offers a caution to civil libertarians. After a major attack, lawmakers will reach for, and will have the political capital to enact, the templates developed beforehand—whether or not civil libertarians signed off on them. Indeed, during 2015's interagency debate, the Intelligence Community apparently used this prospect as an argument against permanently forswearing mandatory-decryption legislation. Robert Litt, General Counsel for the Office of the Director of National Intelligence, reportedly wrote in an internal email that

while "the legislative environment is very hostile today … it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."[34]

This suggests that civil libertarians should engage as these templates are developed—even if their ideological pre-commitments prevent them from doing so publicly, and even if they are ultimately (and legitimately) unwilling to sign off on the final product. Whatever influence they can exercise, it is ultimately better for civil liberties, and for the country, if those drafting these legislative templates benefit from their input.

Finally, a word about the role of commissions and other outside bodies. This type of preparatory study need not be done by an outside commission, as the encryption-related efforts of the Senate Select Committee on Intelligence and the House Judiciary Committee illustrate.[35] Sensitive value judgments, as opposed to fact-finding, should be made by Congress rather than unelected commissioners. On the other hand, independent inquiries can establish a shared factual record for legislators to consult. Commissions can also enrich public debate by providing responsible transparency around classified subject matter—the *9/11 Commission Report* and the Privacy and Civil Liberties Oversight Board's report on Section 702 are prime examples.

Commissions have one additional virtue—one that should appeal to those who fear hasty, government-empowering post-attack legislation. If an attack occurs, a pending commission can serve as a buffer against a precipitous response. This is both because Congress will naturally want to benefit from the commission's findings before legislating, and because the commission will provide an alternative focal point for the enormous post-attack urgency felt by the public and Congress.

Anticipating the Day After

In 2005, former Senator Sam Nunn (D-GA) posed two questions that encapsulate the dilemma facing counterterrorism policymakers: "The day after an attack," he asked, "what would we wish we had done? Why aren't we doing it now?"[36] Nunn meant this as a call to arms, but it could equally be the *cri de coeur* of the farsighted but unheeded policy expert. Unfortunately, it is a consistent feature of our political system that we struggle to enact needed reforms until after a galvanizing event. Countercyclical approaches like those described here can perhaps mitigate the cyclical politics of counterterrorism. But not even the most prudent, farsighted efforts can eliminate them altogether. In the age of terrorism, these dynamics will shape our national security response for years to come.

Notes

1. National Commission on Terrorist Attacks upon the United States, Thomas H. Kean and Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004), pp. 260-261.
2. *Ibid.*, p. 208.
3. *Ibid.*, p. 209.
4. Quoted in Gerald F. Seib, "In Crisis, Opportunity for Obama," *Wall Street Journal*, November 21, 2008, https://www.wsj.com/articles/SB122721278056345271.
5. James Madison, *Federalist* No.10, in *The Federalist Papers*, ed. Clinton Rossiter (New York: New American Library, 1961). See also James Madison, *Federalist* No.10.
6. *Authorization for the Use of Military Force*, Public Law 107-40, § 2(a), 107th Cong (emphasis added).
7. See *Report on Associated Forces* (July 2014), available via the ACLU at https://www.aclu.org/foia-document/report-associated-forces.
8. See Ilan Goldenberg et al., "Remodeling Partner Capacity, Maximizing the Effectiveness of U.S. Counterterrorism Security Assistance," Center for a New American Security, November 14, 2016, pp. 6-8, https://www.cnas.org/publications/reports/remodeling-partner-capacity.
9. See The White House, "Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations," December 2016, pp. 5-6; see also Respondents' Memorandum Regarding the Government's Detention Authority Relative to Detainees Held at Guantanamo Bay, Guantanamo Bay Detainee Litigation, Misc. No. 08-442, at 2 (D.D.C. March 13, 2009). The latter argues that the 2001 AUMF covers "associated forces" of the Taliban and al Qaeda.
10. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Public Law 107-56, § 215, 107th Cong.
11. *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, Public Law 114-23, 114th Cong.
12. Jack Shafer, "Why the Underwear-Bomber Leak Infuriated the Obama Administration," Reuters, May 16, 2013, *at* http://blogs.reuters.com/jackshafer/2013/05/16/why-the-underwear-bomber-leak-infuriated-the-obama-administration/.
13. *9/11 Commission Report*, p. 341.
14. *The New York Times*, CBS News, Poll, June 20-22, 2014, http://graphics8.nytimes.com/packages/pdf/jun14d-all.trn.pdf.
15. Julie Hirschfeld Davis and Dalia Sussman, "Obama Faulted in Terror Fight, New Poll Finds," *The New York Times*, September 17, 2014, https://www.nytimes.com/2014/09/18/us/politics/for-first-time-most-americans-disapprove-of-obamas-handling-of-terrorism.html?_r=0.
16. Barbara Starr and Renee Marsh, "AQAP trying to hide explosives in laptop batteries, official says," CNN, Mar. 22, 2017, http://www.cnn.com/2017/03/21/politics/electronics-ban-devices-explosives-intelligence/.
17. *9/11 Commission Report*, p. 357.
18. See, e.g., *9/11 Commission Report*, pp. 103-104 (detailed plan for Afghan tribal operation against bin Laden at Tarnak Farms scratched in May 1998 because of fear of collateral

damage), 188 (proposal to set up clandestine CIA base in northern Afghanistan "was turned down as too risky" in 2000).

19. William Johnstone, *9/11 and the Future of Transportation Security* (Greenwood Publishing Group, 2006), p. 43.
20. Frances Larson, "What a beheading feels like: The science, the gruesome spectacle — and why we can't look away," Salon, February 3, 2015, http://www.salon.com/2015/02/03/what_a_beheading_feels_like_the_science_the_gruesome_spectacle_and_why_we_cant_look_away/.
21. Philip Zelikow, "Afterword: The Twilight War," in *The 9/11 Commission Report: The Attack from Planning to Aftermath*, authorized text, shorter edition, (Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2011), p. 510.
22. Institut Français d'Opinion Publique, *Le regard des Français sur les grands enjeux de l'élection présidentielle: La sécurité #3*, March 2016, p. 16, http://www.ifop.com/media/poll/3691-1-study_file.pdf.
23. See Charlie Savage, *Power Wars: Inside Obama's Post-9/11 Presidency* (New York: 2015), pp. 77-78, 95-97.
24. *Al-Aulaqi v. Obama*, No. 1:10 CV 01469 (D.D.C. Dec. 7, 2010).
25. *9/11 Commission Report*, p. 104.
26. *See* [Untitled] White Paper on Approaches to Encryption, https://assets.documentcloud.org/documents/2430092/read-the-obama-administrations-draft-paper-on.pdf; see also Andrea Petersen and Ellen Nakashima, "Obama Administration Explored Ways To Bypass Smartphone Encryption," *Washington Post*, September 24, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html.
27. Adam Klein et al., *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond*, Center for a New American Security, p. 43 (Dec. 2016).
28. *See* Adam Klein, *Decryption Mandates and Global Internet Freedom*, Hoover Institution Aegis Paper Series No. 1608, pp. 14-15 (2016).
29. Josh Lepchitz, "Cybersecurity Information Security Act: How a Contested Bill Quietly Passed," blog post, *Richmond Journal of Law and Technology*, January 19, 2016, http://jolt.richmond.edu/index.php/cybersecurity-information-security-act-how-a-contested-bill-quietly-passed/.
30. *Reflections on the Tenth Anniversary of The 9/11 Commission Report* (Bipartisan Policy Center, July 2014), p. 17.
31. See Michael Warner and J. Kenneth McDonald, CIA Center for the Study of Intelligence, *US Intelligence Community Reform Studies Since 1947*, (April 2005), p. 22; Office of the Director of National Intelligence, Frequently Asked Questions, at https://www.dni.gov/index.php/about/faq.
32. See, e.g., *To authorize the use of United States Armed Forces against al Qaeda, the Islamic State of Iraq and the Levant (ISIL), and the Afghan Taliban*, H. J. Res.114th cong., 1st Sess., draft legislation released by Rep. Adam Schiff, available at: https://www.justsecurity.org/wp-content/uploads/2015/12/SCHIFF_023_xml.pdf; Robert Chesney et al., "A Statutory Framework for Next-Generation Terrorist Threats," Jean Perkins Taskforce on National Security and Law, Hoover Institution, February 25, 2013, http://www.hoover.org/research/statutory-framework-next-generation-terrorist-threats; S. 1587, 114th. Cong. (2015); *To authorize the use of United States Armed Forces against al Qaeda*, H. J. Res.

33. *Compliance with Court Orders Act of 2016*, discussion draft, BAG 16460, 114th Cong., 2nd Sess., https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf; see also "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill," press release, from Sen. Dianne Feinstein, April 13, 2016, https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649.
34. Ellen Nakashima and Andrea Peterson, "Obama faces growing momentum to support widespread encryption," *The Washington Post*, September, 16, 2015, https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html?utm_term=.e853c4d17e81.
35. See supra note 33; House Judicary Committee and House Energy and Commerce Committee, *Encryption Working Group Year-End Report*, December 20, 2016, https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf.
36. Sam Nunn, Co-Chairman, Nuclear Threat Initiative, "The Day After an Attack, What Would We Wish We Had Done? Why Aren't We Doing It Now?" Statement before the 9/11 Public Discourse Project, June 27, 2005, http://www.nti.org/analysis/testimonies/day-after-attack-what-would-we-wish-we-had-done-why-arent-we-doing-it-now/.