GEORGETOWN UNIVERSITY PRESS

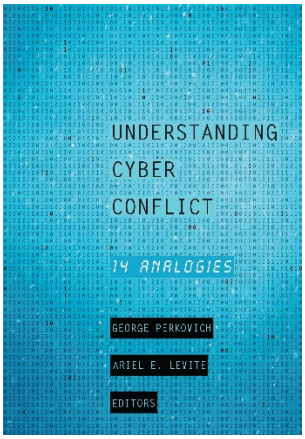
Cyber, Drones, and Secrecy

David E. Sanger

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



For additional information about the book:

http://press.georgetown.edu/book/georgetown/understanding-cyber-conflict

4 Cyber, Drones, and Secrecy

DAVID E. SANGER

The week before Barack Obama first took the oath of office as president of the United States in January 2009, he entered the Oval Office for one of those great traditions of American democracy, the moment when the president-elect meets with the sitting president for a candid conversation about the global realities he is about to face.

There was very little that Obama and George W. Bush liked about one another. Obama had been elected on a platform of extracting America from what he once called "dumb wars" of occupation. Bush, in Obama's thinking, had two traits that did not go well together—an absence of intellectual curiosity, which led him to take questionable intelligence that crossed his desk at face value, and an overtendency to reach for military force when it came to exerting American power. To Obama the 2008 election had been a referendum on the wars in Iraq and Afghanistan. To Bush, Obama's election was symbolic of a nation that still could not face the hard lessons of the September 11, 2001, attacks; particularly, he felt America had to think differently about conducting an aggressive, anticipatory, and sometimes preemptive defense.

But in their meeting that day, Bush told his successor that, politics aside, there were two programs he would be foolish to abandon, because they could both protect the nation and potentially save his presidency. The drone program was, by that day in 2009, the least covert program in the arsenal of counterterrorism measures of the Central Intelligence Agency (CIA). The agency used armed, remotely piloted vehicles to wipe out small clusters of militants as they plotted against US forces in Pakistan and Afghanistan. The use of drones, while still limited, surged during the Bush administration. When the 9/11 attacks happened, drones had been entirely a surveillance platform, and their utility had been largely dismissed by the US Air Force, which never viewed unmanned aerial vehicles (UAVs) as real airplanes since they were not flown by pilots who put their lives at risk. Necessity changed this way of thinking. The Predator and ultimately its much larger cousin, the Reaper, were equipped with missiles that could wipe out a living room full of suspected terrorists and usually keep the house next door untouched. Use of the Predator was limited in Bush's early days

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

in office, with the relatively small fleet divided between the Iraqi and the Afghan-Pakistani theaters. But by the time of Obama's inauguration, the planes were rolling off the production line.

The second program the two men discussed in that meeting was, in contrast, perhaps the most covert program in the US government and known only to a very tight group of aides. It was code-named Operation Olympic Games. Obama knew a bit about it from his security briefings as a candidate, but he had not been immersed in the details. He was about to be.[1]

Olympic Games was the first truly sophisticated offensive cyber operation in American history. Like armed drones, cyber weapons had been born of necessity—in this case, the need to slow the development of Iran's nuclear program. It had been the brainchild of a fledgling offensive cyber operation built within US Strategic Command, a unit better known for tending to America's strategic nuclear weapons, and of cyber operators at the National Security Agency. Later, the CIA would play a larger and larger role. But unlike with drones, the success of the Olympic Games operation was far more uncertain.

The first tests were promising. A "worm" was inserted into the computer controllers that commanded the operation of centrifuges inside the Natanz nuclear enrichment center. By 2009 the worm was already succeeding at speeding up and slowing down the supersonic machines, sending them spinning out of control. Best of all, the Iranians had not figured it out. Unlike the targets of drone operations, they did not know they were under attack, though some harbored suspicions. But the effects so far had been limited; without a doubt, they were less dramatic than a drone strike.

In his first year in office, Olympic Games became the vehicle for Obama's primer in America's nascent offensive cyber capabilities. From the same newly renovated Situation Room where he reviewed the details of the drone program, the new president examined, time and time again, a giant schematic of the Natanz nuclear enrichment plant spread out before him. A range of officials—intelligence officers, generals, lawyers—circulated in and out and explained how the most sophisticated new weapon in the American cyber arsenal, later dubbed Stuxnet, was being aimed at critical clusters of centrifuges in Iran's nuclear program. The operation had been developed in concert with Israel's Unit 8200; indeed, when details leaked in 2012, Israeli officials, while not publicly acknowledging the effort, privately took credit for its success. In fact, some Israelis contended that they were more responsible for the operation's development than were officials in Washington.[2]

Whatever the origin, Olympic Games was seen in Washington as an alternative to bombing Iran's nuclear facilities, and to the Americans it was a way of focusing Israel's energies on a project that promised to slow Iran's progress with a limited risk of triggering yet another Middle East war. And yet, as in the drone program, there was a deep sense of the experimental nature of the enterprise. Cyber weapons had been used before but largely in computer-on-computer attacks. No one could remember a case where an American president oversaw a cyber attack on physical infrastructure, hoping that it could accomplish what

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

previously would have required bombs or saboteurs. As with the drone program, every debate about how and when to deploy America's cyber capabilities, and under what rules of engagement, seems to carve new territory.

Today as President Trump has taken over far more mature drone and cyber programs, clearly the two weapons raise similar moral and legal issues that future presidents will have to grapple with. Indeed, Pentagon officials openly wonder whether the next major global conflict might open in cyberspace and be prosecuted by a range of new, autonomous weapons—not only aerial unmanned vehicles but also undersea ones. And yet these drone and cyber weapons, nurtured by the same policymakers and sometimes used in the same conflicts, have taken very different paths—as have the questions surrounding their use.

The drone became President Obama's weapon of choice, as an alternative to sending troops into areas of the world that Obama feared would become quagmires. He used drones in Pakistan against al Qaeda, in the Horn of Africa against al-Shabaab militants, in Yemen against a variety of extremist groups, and in Iraq and Syria against the Islamic State. In most of those cases, the CIA conducted the attacks under Title 50 authority, which outlines the authorities for "covert action." Thus, the United States could not acknowledge the strikes, and any rules of engagement would also be kept secret. Obama, in a candid discussion with law students at the University of Chicago in April 2016, conceded that this did a "disservice" to the creation of legal and ethical standards for the strikes, something he said he was trying to repair.[3]

In those same comments, Obama acknowledged that in his first years in office he was concerned that the drone program had a weak legal basis. He had never suggested it at the time as the administration alternated between ducking questions about the program and simply defending its use.

"I think it's fair to say that in the first couple of years of my presidency, the architecture—legal architecture, administrative architecture, command structures—around how these [strikes] were utilized was underdeveloped relative to how fast the technology was moving," he said. He told the students that he pushed his staff to come up with a complex set of rules and legal strictures to make sure each strike comported to the rules of law—that is, that they amounted to a proportionate use of force, that civilian casualties were limited, and that the United States was not creating as many or more adversaries as it was killing.[4] As the program sped ahead and emerged from the shadows, Obama made an effort, one that only partially succeeded, to move more of the program out of secret intelligence channels and more into the hands of the US Air Force, where strikes and their adherence to law could be more openly debated. Near the end of Obama's presidency, National Security Adviser Susan Rice, in a speech at the US Air Force Academy in Colorado Springs, thanked the academy for turning out a new generation of combatants with an understanding of the rules that governed this new weapon and with an ability to handle the many stresses of using it.[5]

It is not clear that Obama and Rice could have given the same set of speeches about cyber weapons, which they discussed far less frequently. Indeed, though cyber weapons can usually be employed in a far less lethal manner than guided

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

missiles shot from a drone, they have been deployed less frequently and under rules of engagement that are far less clear, at least to the public. Indeed, the rules for cyber weapons have seemed more difficult to develop, for the effects of a cyber strike are not as predictable as those for drone strikes.

These differences have given rise to one of the many oddities in the way governments and policymakers think about employing drones and employing cyber weapons. Since 2004, armed drones have been aimed at killing people, mostly suspected terrorists. Cyber weapons, in contrast, have been focused on an adversary's weapons systems, facilities, and equipment that can be repaired. One would think that given the difference in lethality, there would be more hesitance to use a drone than a cyber weapon. Oddly, exactly the opposite has been the case.

Why is that? Perhaps drones seem to be an extension of any other kinetic weapon, although they unleash more precisely targeted bombs and thus may seem a more humane way to execute a military or covert operation. But the answer may also have to do with the unpredictability of cyber attacks. The concerns about what could go wrong—the possibility that code could escape and wreak havoc on a broad swath of civilians while perhaps only temporarily disabling its intended target—almost paralyze cyber operators. The president had to intervene in the fall of 2015 to get the US Cyber Command to turn its digital guns on the country's number one terrorist enemy at the time, the Islamic State.

The Islamic State example is a telling one. Mr. Obama and his staff talked about those attacks because they took place in an environment that seemed closer to traditional war than to covert action. And in a war, the law of armed conflict frames the choices. Decision makers may be more cautious and more restrained than required under the law, but the rules of war create limits. US Cyber Command constantly holds meetings to assess whether the use of cyber weapons complies with the principles of necessity, discrimination, and proportionality—that is, the rules that would apply in the case of an armed attack.

But in peacetime, or in times of confrontation that have not yet turned to open conflict, calculating what types and levels of coercion are legitimate is far more difficult. This creates a political and strategic challenge as much as a legal and tactical one. Conducting attacks with drones or malware that seem shocking, callous, unfair, misdirected, or damaging to "bystanders" can easily sow backlash at home or inside friendly states. It can spur terrorist recruitment, and it can encourage retribution. The choices framed in this chapter assume that most cyber attacks, like most drone attacks, will take place in the gray area between declared state-on-state war and peacetime operations. In short, the decisions President Donald Trump will have to make will likely be similar to the vexing choices Mr. Obama faced on whether to use cyber weapons as an alternative to more traditional forms of low-level warfare, even while recognizing that, sooner or later, that may escalate the global use of cyber weapons. Only at the end of the Obama administration was it possible to start comparing the issues, and lessons, raised by using drones and cyber weapons. Much more analysis will likely be possible years from now, as details of the two programs are declassified

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

or leaked, but now one can reach some tentative conclusions, rooted in the early histories of both programs.

The Light-Footprint Strategy

From the early years of the Obama administration, these two weapons—drones and cyber—became keystones of what is known as the "light-footprint" strategy. (The third element was the increased reliance on special operations forces.) Both drones and cyber weapons allowed for remote-control attacks, which are politically attractive in a country tired of casualties from two grinding ground wars. Both weapons were stealthy. Both were cheap, at least by the standards of a Pentagon burning through more than $600 billion a year. That combination soon made them as irresistible to Obama as they had been to his predecessor. The low cost meant that the president could experiment with them without needing a big appropriation from Congress. Moreover, they were swathed in secrecy, meaning, among other things, that it was still possible to hide mistakes.

They were also, as Obama would soon learn, capable of redefining a president's view of how to exercise military power. Obama reserved to himself the right to authorize the use of both weapons. By 2012 the president was personally overseeing the "kill list," the list of potential human targets for the drones. He was also overseeing the first use of cyber weapons and worrying about the precedents that he was setting for a new age of cyber conflict, one in which America would be vulnerable.

Yet how these two programs were viewed and employed would diverge during the Obama presidency. Drones became caught up in a political firestorm. At home it became clear that the "clean" kills of these precise weapons often involved considerable collateral damage, a fact the Obama administration went to some lengths to downplay. The remote-control nature of the killings raised moral and ethical questions, some voiced by former UAV pilots. And America's monopoly on the technology—and thus its ability to set some norms about their use—faded as other countries raced to match the US drone capability. Israel and China both have advanced programs; most others are still catching up.

Cyber attacks, because they are so stealthy and their effects often so hard to see, were treated more as a state secret—and were less politically charged. But the barrier to entry for other countries was low, and as Obama entered the twilight of his presidency, many sophisticated players existed. Olympic Games proved to be the start of a new era of state-sponsored cyber attacks. Seven years after Obama's meeting with President Bush, Russia, China, North Korea, and Iran had all launched state-sponsored attacks and had become far more skilled at cyber exploits and espionage.

The policy of secrecy surrounding the drone and cyber programs diverged as well. The administration wisely gave up its futile effort to avoid talking about drones; since each attack was reported in the media, the technology was not deniable. In the White House press room, where officials had been instructed by

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

lawyers not to discuss drones at all, or at least not those operated by the CIA, the fiction that the weapon did not exist gradually faded. By 2013 the president himself had delivered a detailed speech about the legal basis for the drone program and had joked about the weapon on a late-night comedy show and at the 2010 White House Correspondents Dinner. His administration worked to develop what one aide called a regular order of procedures and considerations about using the unmanned, remotely piloted killing machines—and of special rules for when they were used, in rare cases, against an American citizen. The president, in short, was trying to get out ahead of the public debate, to define a set of rules for a new era of conflict, and to normalize use of the weapon for his successor.

But he could not—or at least did not—do the same for cyber. Other than acknowledging, almost in passing, that the United States makes use of offensive cyber weapons, he refused to discuss them in public, save for acknowledging in 2016 that cyber weapons were being employed against the Islamic State. (His last deputy secretary of defense, Robert Work, even went to some rhetorical lengths when he told reporters that the United States was "dropping cyberbombs" on the extremist group, an effort to analogize the imagery of kinetic activity to what appeared to be fairly standard efforts to disrupt the command-and-control mechanisms of the jihadist group.)[6]

When cyber capabilities were discussed, it was in the vaguest terms. The whole technology was still considered to be classified. To this day, Olympic Games has never been officially acknowledged, nor have the lessons of its successes and failures been publicly debated. The result is a stilted conversation that impedes debate about how, when, and under what authorities the United States could use cyber weapons. Worse yet, there is little public debate of how to develop a doctrine for both deterrence and offensive uses. The admiral who commands both the National Security Agency and US Cyber Command—the heart of the offensive cyber weapons effort—conceded in many public forums that the United States was still struggling to develop a theory of cyber deterrence that is analogous to the deterrence theory that surrounds nuclear weapons. In short, the United States found itself, at the time of this writing, still unable to do what it managed to accomplish in the nuclear age: keep the details of the weapon itself classified but hold a vibrant, unclassified debate about its use.

To understand the commonalities and the differences in American debates over how to use drones and cyber weapons, it is first necessary to consider how the weapons differ.

A Short History of Drones and the Myth of Perfect Aim

It did not take long for Obama to embrace his predecessor's advice to retain and accelerate the two secret programs.

For a new president seeking a way out of Iraq and debating a brief surge in Afghanistan, drones were particularly attractive. The more Obama learned about the technology, the more he turned to it. The first term of his administration saw

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

about three hundred drone strikes in Pakistan alone, roughly a sixfold increase from the number during the entire Bush administration.

The increase was striking. But it did not become an issue in President Obama's re-election bid in 2012, and that alone is telling. Obama's liberal base preferred to ignore that the man they elected to change the course of American national security had embraced a vivid symbol of the Bush era. The right wing, which wanted to portray Obama as a "community organizer," did not want to cite evidence that he was using the drone as a killing machine more frequently than his predecessor had. Since it fit no one's preferred electoral narrative, it was rarely an issue.

My *New York Times* colleague Charlie Savage put the appeal of the UAVs quite well in *Power Wars*, his study of the legal struggles of the Obama administration to create a legal framework for these new weapons:

> Under Obama, remote-controlled aircraft were becoming the weapon of choice for strikes away from the traditional battlefields. In part this is because he had far more of them to deploy than Bush had had—the technology was brand new and it had taken time to ramp up production. But Obama was also enraptured by their potential for risk reduction. Conventional air power strikes put American pilots—and sometimes Special Operations spotters on the ground—at risk. By contrast, if a drone crashed or was shot down, its pilot still went home for dinner. They also enabled operators to watch a target for a long period before unleashing a missile, which held out the promise of greater precision and fewer civilian deaths.[7]

That set of qualities in the drone—its clandestine operation (with the attendant plausible deniability and limited oversight), casualty-free nature (for the attacker), persistence over the target, and apparently dead-true aim—was both attractive and deceiving. Persistence allowed a pilot with a joystick somewhere in the Nevada desert to watch a target for days, but it also offered false confidence that the trigger would be pulled at just the right time. Often it was not. American efforts to dispute the existence of collateral damage soon collapsed under further study.

The trouble became particularly acute after the Bush administration authorized "signature strikes" in 2008. No longer would drone operators have to hunt an identified individual terrorist or militant. Instead, a motorcade that appeared to be carrying a group of Taliban or al Qaeda militants became a legitimate target, even if there was no great certainty about who was inside the cars.[8] So would a gathering in which a terror suspect met with colleagues, even if the latter were unknown to the drone operator. When my colleague Eric Schmitt and I first reported on this change in policy, in which "patterns of life movement" made for new target sets, our story explained why the pace of strikes rose so quickly during the last months of the Bush administration and at the beginning of the Obama administration: the weapon had moved from one used for "targeted killing" to one used for protecting the US military.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

But the wider use of signature strikes created problems similar to the attribution problem that plagues the investigation of cyber attacks. By definition, the intelligence surrounding a signature strike is imprecise. That motorcade could be full of al Qaeda terrorists. Or it could be full of teenagers or guests for a wedding. In the cyber realm, it is difficult to imagine that the president would allow a strike against, say, a Chinese computer server simply because an attack on the Pentagon looked typical of Chinese behavior. It could, in fact, be an elaborate ploy. Yet in the drone world, the United States was essentially doing exactly that—striking cars that moved in ways "typical" of al Qaeda. No wonder Obama expressed misgivings about the rules of engagement.

Signature strikes quickly raised questions about the standards of intelligence used to authorize an attack. Precisely because the identities of the targeted individuals were unknown, the success of the missions became far harder to measure and often far more dubious. Collateral damage soared. By one outside estimate, 482 drone strikes in Pakistan, Afghanistan, and Yemen resulted in around 289 civilian casualties.[9] And even after a strike the CIA oftentimes had no idea who some of the occupants in the motorcade or a meeting actually were.

This posed both a statistical and a political problem: suddenly the precision killing tool looked less precise. The solution was a piece of statistical innovation. Soon all males older than grade-school age who were killed in a strike were counted as "presumed combatants," even if their identities were unknown.[10] As intended, this vastly lowered the collateral damage statistics. In congressional oversight hearings and in speeches, the UAV was once again described as an instrument of remarkable wartime precision.[11]

Of course, in places like Pakistan the level of resentment against drones soared. Pakistani media often exaggerated the collateral damage and failed to report the killing of true militants and terrorists. At other times, misjudgment by American operatives led to tragedy. Local tribesman told stories of an attack on a *jirga* (assembly) at which some Taliban members came to act as mediators: when the drone-launched missile struck, the Taliban died, and so did many of the tribal elders. Over time the drone became the symbol of an aggressive, heartless America, its image sketched out in markets in Peshawar. Its constant overhead buzz, with its suggestion of imminent death and wreckage, became associated with a distant power that did not know how to control the weapon in its hands.

One such strike resulted in a considerable tightening of the targeting roles. After a minor rebellion in the Obama war cabinet, led by Secretary of State Hillary Clinton and Chairman of the Joint Chiefs Adm. Michael Mullen, the administration concluded that the signature strike standard was simply too loose.[12] American ambassadors were given far more authority to sign off on—or halt—a strike in "their" territory, an imposition of State Department control that quickly resulted in serious conflicts with the CIA and the Pentagon. The latter agencies were not accustomed, or very happy, with the idea of career foreign service officers limiting their ability to pull the trigger.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

Over time, Obama himself became deeply involved in debating what was a legitimate target and what was not, a subject that appealed to his legal training but also left him feeling deeply uneasy. My colleagues Scott Shane and Jo Becker captured this in a story about the president's direct role in approving the kill list, or those targeted for assassination from the air.

> Mr. Obama is the liberal law professor who campaigned against the Iraq war and torture, and then insisted on approving every new name on an expanding "kill list," poring over terrorist suspects' biographies on what one official calls the macabre "baseball cards" of an unconventional war. When a rare opportunity for a drone strike at a top terrorist arises—but his family is with him—it is the president who has reserved to himself the final moral calculation.
>
> "He is determined that he will make these decisions about how far and wide these operations will go," said Thomas E. Donilon, his national security adviser. "His view is that he's responsible for the position of the United States in the world." He added, "He's determined to keep the tether pretty short."[13]

In an interview late in his presidency, Obama reflected on how American leaders found themselves making these life-and-death decisions from conference rooms in Washington. It started, he said, with the best of intentions after 9/11. Referring to both the military and the CIA, he noted that "they started just going because the goal was let's get al Qaeda, let's get these leaders. There's a training camp here. There's a high-value target there. Let's move."

Obama then went on to offer the most detailed explanation any American president has given of the kind of structure he tried to impose around the rules of engagement for using of drones:

> Given the remoteness of these weapons and their lethality, we've got to come up with a structure that governs how we're approaching it. And that's what we've done. So I've put forward what's called a presidential directive. It's basically a set of administrative guidelines whereby these weapons are being used.
>
> Now, we actually did put forward a non-classified version of what those directives look like. And it says that you can't use these weapons unless you have near certainty that there will not be civilian casualties; that you have near certainty that the targets you are hitting are, in fact, terrorist organizations that are intending to do imminent harm to the United States. And you've got all the agencies who are involved in that process, they have to get together and approve that. And it goes to the highest, most senior levels of our government in order for us to make those decisions.
>
> And what I've also said that we need to start creating a process whereby this—whereby public accountability is introduced so that you or citizens or

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

members of Congress outside of the Intelligence Committee can look at the facts and see whether or not we're abiding by what we say are these norms.

And we're actually—there's a lot of legal aspects to this because part of the problem here is, is that this drone program initially came through the intelligence side under classified programs, as opposed to the military. Part of what I've also said is I don't want our intelligence agencies being a paramilitary organization. That's not their function. As much as possible this should be done through our Defense Department so that we can report, here's what we did, here's why we did it, here's our assessment of what happened.

And so slowly we are pushing it in that direction. My hope is, is that by the time I leave office there is not only an internal structure in place that governs these standards that we've set, but there is also an institutionalized process whereby the actions that the U.S. government takes through drone technology are consistently reported on, on an annualized basis so that people can look.

And the reason this is really important to me—and this was implied in your question—is there is a lot of misinformation about this. There is no doubt—and I said this in an interview I think recently—there is no doubt that some innocent people have been killed by drone strikes. It is not true that it has been this sort of willy-nilly, let's bomb a village. That is not how folks have operated. And what I can say with great certainty is that the rate of civilian casualties in any drone operation are far lower than the rate of civilian casualties that occur in conventional war.[14]

Does Obama's Drone Standard Work for Cyber Strikes?

Obama's explication of how he tried to develop rules for the use of drones is worth considering as parallel questions are addressed on the use of cyber weapons.

The initial parallels are striking. In the debate over Olympic Games, Obama showed a similar concern over making sure "you can't use these weapons unless you have near certainty that there will not be civilian casualties." He wanted to ensure that local Iranian hospitals, for example, were not taken out along with the Natanz centrifuges. He succeeded in avoiding such a scenario in that case, but in many other cases where cyber will be most useful—for example, taking out a power grid or a cell phone network—the ultimate effects are unpredictable and could well result in the loss of civilian lives.

In cyber attacks, the decision-making also "goes to the highest, most senior levels of government." Under existing directives, only the president can authorize offensive cyber strikes in both peacetime and wartime. Of course, reality is more complicated. Is a preventive or preemptive effort to block an attack on the United States—say, by taking out a server in China or North Korea—an "offensive" strike? Or is it simply "active defense," even if it looks to the target country like an act of offense?

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

But one of Obama's standards—that the "targets you are hitting are, in fact, terrorist organizations that are intending to do imminent harm to the United States"—does not fit at all. That criterion clearly did not fit the Iran case. Its government might be a state sponsor of terror, but it was not a terrorist organization. Its drive to produce a nuclear weapon was a threat to the United States but not an imminent one, for it was months, if not years, away. (The cyber attacks on the Islamic State, of course, were far more in line with the Obama test for drones.)

In fact, the drone standard laid out by Obama may be of only limited use when applied to cyber conflict. And it is worth remembering that cyber capabilities have some unique advantages over drones:

- Cyber strikes can be dialed up and dialed back; thus, the level of damage is, theoretically, much easier to control.
- Most cyber strikes do not necessarily lead to fatalities.
- If the strike is well hidden, it is entirely possible that the same target can be hit repeatedly, giving the president the option of starting with a small attack and increasing the level as needed.
- Not only is a cyber strike more plausibly deniable than a drone strike, it is possible to make it look as if someone other than the true attacker is responsible. For that reason, the levels of transparency that President Obama ultimately sought to achieve for US drone operations would likely be resisted by both the Pentagon and the intelligence community.

This last difference is worth a bit more consideration. The availability of outright secrecy surrounding cyber strikes—or, at a minimum, plausible deniability—may create an incentive particularly for intelligence agencies to use the weapon more aggressively. So far there is no way to measure that accurately from the outside, as no records of how many cyber strikes take place (and definitions of a "strike" would likely vary) and no discussion of what percentage of proposed strikes are actually executed are made public. Some anecdotal evidence suggests a reluctance to conduct cyber strikes because the code could act in unpredictable ways and perhaps reveal the identity of the country that launched it. It is a legitimate fear, for that is exactly what happened in the case of Olympic Games.

In short, one significant disadvantage of using cyber weapons is that the results can be significantly more unpredictable than many advocates of the technology admit. The immediate impact is difficult to assess because so much depends on the inner workings of the target and the quality of the intelligence about that target. Further, its long-term consequences are almost impossible to anticipate. Code mutates. It is cut up into smaller pieces and used for other purposes. The list of what can go wrong—or at least of what is unexpected—is a long one.

Moreover, the experience with drones has made some in Washington worry about the international reaction if the United States is linked to an attack on a state. Drones fostered the image of the United States as an uncaring superpower

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

using its technological edge to rule the world; cyber attacks could make it look callous should they affect a power grid or a hospital. (American officials found it easier to boast about cyber attacks on the Islamic State for a few reasons: the target group is widely reviled, and because it has no real infrastructure of its own, apart from stolen oil rigs, an attack carried little risk of worsening the lives of ordinary Iraqis and Syrians.)

It is not clear whether the ability to cloak the identity of the cyber attacker encourages nations to conduct attacks or whether the fear of revelation acts as a brake. The latter appears to have held sway, according to anecdotal evidence, in some cases when the US Cyber Command drew up plans for possible attacks. Doubtless the calculus is different in every case. As one senior American official told the author, "If we are aiming at a state, with all the questions of violating sovereignty, the standards for assuring you can act covertly are much higher."

Geography Still Matters

In the run-up to the Iraq War in 2002, George W. Bush gave a set-piece speech in the grand hall of the Cincinnati train station, warning of the evils Saddam Hussein could impose on the United States.[15] Many shaded truths in the speech were worthy of question, especially in retrospect. But even at the time, one section appeared particularly fanciful. Bush raised the specter that the Iraqi leader would float a ship off the coast of the United States and launch an attack with a secret fleet of UAVs armed with chemical or biological weapons that could be dropped on American cities. The idea never quite garnered the ridicule it deserved, for the ship would have been a sitting duck for the US Coast Guard or the navy, and biological and chemical weapons are hard to disperse effectively. But the imagery of a flotilla of drones illustrates the first significant difference between drones and cyber: with drones, geography still matters, as it limits the weapon's effectiveness.

Fourteen years after that speech was delivered, it is still hard to imagine how a foreign power could launch such an attack. A base near the United States would be necessary, and, of course, hiding such an air base would be difficult. Thus, the Bush administration needed to conjure up a ship-based solution to the problem.

Cyber capabilities, in contrast, defy all geographic limits. Had he possessed the coding talent, Saddam Hussein would have been able to launch cyber attacks from one of his garish palaces. (He never seemed interested, but perhaps he would have been if he had survived another decade.) Moreover, cyber attacks are much easier to hide than a fleet of UAVs. Attacks can emanate from a People's Liberation Army tower in Shanghai, from a cell of North Koreans operating in Thailand, from a bot reproducing itself on Grandma Smith's home computer in Des Moines, or from a university in the American South. In fact, each of those places has been the source of attacks seen in the United States since 2012.

Certainly, the ability to detect such cyber threats—addressing the "attribution problem"—has come a long way in recent years. Walking into the Department of Homeland Security's giant, space-age-looking command post in suburban Virginia,

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

it looks like a flight control center, with screens monitoring levels of Internet activity and malware across the nation. In the case of the North Korean attack on Sony Pictures Entertainment in late 2014, it took US intelligence agencies only a few days to conclude with high certainty who the attackers were. (That process was aided by the fact that the United States had pierced North Korea's networks, for other reasons, four years before and could detect post facto evidence of the attack in its systems.) Figuring out the source of attacks on banks that use the SWIFT banking system took longer although some of the code appeared to be very similar to what was used against Sony. In that case, the US government was more cautious. It was all a reminder that in the cyber realm, attribution remains as much art as science.

For now cyber can create a much larger swath of destruction than can drones, though the effects of a cyber attack are more reversible, or at least fixable, than those of a drone strike. That may not remain true for long. Eventually drones may be capable of being armed with weapons of mass destruction of some form, but the very thing that makes drones stealthy—their ability to fly "under the radar"—also currently makes them too small to carry much punch. So today they pose a direct threat to small clusters of terrorists and to commercial aviation. Their ability to create mass casualties is limited. In short, drones are a containable problem—or at least a manageable one. For a foreign state, they are not a weapon of choice: their range is too limited, and over time the chances of discovery are high. For a terrorist seeking to do high-publicity damage, it is cheaper and easier to mount an automatic weapons attack.

Cyber capabilities, in many ways, pose the opposite problem. The oceans and wide spaces that give America protection from an overwhelming attack of UAVs offer no such protection in the cyber realm. From a keyboard in Moscow or Shanghai, Pyongyang or Tehran, the world is borderless, and information travels nearly instantaneously. No local crews are needed to maintain the weapon or refuel it. If adjustments need to be made to the weapon, the work can be done from half a world away. As one cyber warrior put it, "With cyber you don't have a Djibouti problem"—a reference to the problem of negotiating, then maintaining, a launch base in a faraway nation. All cyber war can be distant, yet its effects can be local.

Even if an attacker is identified with high certainty, however, the barriers to taking preemptive defensive action remain extremely high and even far higher, at least for now, than if the United States saw a physical attack massing on the border. Consider these scenarios: If North Korea were to launch a missile in the general direction of the West Coast of the United States, there is little question that the United States would try to shoot it down. (In fact, Defense Secretary Donald Rumsfeld ordered Pacific Command to be ready to do just that when the North Koreans were threatening a launch in 2006.[16]) If Mexico sent an armed drone over the border, undoubtedly the United States would again try to shoot it down. But what if the National Security Agency saw a Sony-like attack massing in a North Korean server or in the computers of a Mexican drug lord? It is far from clear what the US response would be. The Defense Department doctrine on

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

cyber activity states that in certain cases an attack would merit a national response, but the threshold is understandably vague. So is the nature of the response. Would the United States simply block the attack—something companies and virus protection software do every minute of every day? Or would it seek to take out the source, which could be a server, a den of hackers, or a military cyber unit?

The legal debate in the United States about what constitutes a threat worthy of preemption goes back to the missives exchanged by Daniel Webster and his British counterpart after a half-baked scheme to attack Canada resulted in Britain's burning the steamboat *Caroline* in 1837.[17] But the hesitance to, say, fry a server in Shanghai where malware is being assembled to attack an American company raises a new level of complexity. While the armed drone coming over the border is an obvious threat, the code flowing across a fiber-optic cable beneath the sea is not so obvious. The Chinese attacker would doubtless say that the code he sent around the world was benign, and it may, at first glance, appear that way. Proving the code was Chinese, sanctioned by the Chinese government, contained malware, and was intended to do great harm (rather than merely facilitate espionage) would be enormously difficult and likely pit one group of experts against another.

Indeed, it already has. The opening attack on Sony Pictures was an implant that surveyed the company's computer systems, probing its vulnerabilities. For months it acted more like an unarmed drone, interested only in espionage, than an armed one. But once in place and after it had surveyed Sony's weaknesses, the malware turned to another purpose—an attack. In short, it morphed from benign to deadly at the flip of a switch.

No one saw that coming, least of all Sony's leadership. But one senior US intelligence officer told me that "even if we had known in advance what the code could do, it's not clear we would have struck back." It is unclear whether he thought President Obama acted cautiously because of the absence of a smoking gun to prove North Korea culpable or because the administration debated and doubted how aggressively the US government should retaliate for an attack on what was a private entity rather than a public one.

Moreover, when the United States publicly declared North Korea was the culprit, many experts responded it was wrong.[18] The attack wasn't from the North, they said, but from a group of hackers pretending to be under the command of North Koreans. Others said Sony was the victim of hacktivists or teenagers.

It is not surprising that the Pentagon is spending so much time thinking about asymmetric responses to cyber attacks; this retaliation may be of an entirely different nature than counterattacking in the cyber realm. In the case of China, US retaliation came in the form of indicting officers from Unit 61398 of the People's Liberation Army. While it made Justice Department officials feel good, whether it made much difference in Chinese thinking about future attacks is debatable. Some believe that the public shaming chastened President Xi Jinping and other Chinese officials and forced them into an agreement with the United States. Others think that agreement was largely for show.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

In the North Korea–Sony Pictures case, modest sanctions were imposed; it is unclear whether covert action was taken to disable North Korea's limited number of Internet protocol addresses. In other cyber attacks—the Iranian attacks against Saudi Aramco (2012), the Sands Casino and American banks (2014), and even the New York dam (2013)—there has been no noticeable response or at least no public one.[19]

Then another debate faced the Obama administration in developing cyber weaponry: what to do about collateral damage?

In approving the Olympic Games attacks, President Obama asked detailed questions about whether the computer worm could hit a hospital or a school, or whether it could end up taking out the local power grid. He was assured it could not, and there is no evidence of collateral damage resulting from the strikes themselves.

But another unanticipated form of that attack's damage came later. When the Stuxnet worm leaked out, the whole world could see the code that created it. Moreover, it could see the "modules" of the code itself. Many of these modules have served as the building blocks of other weapons, which other people have used in other attacks. One security researcher recently told the author that five years later, "elements of the Stuxnet worm are still being used in other malware." The weapon itself wasn't reproduced. But its parts were.

In short, drones and cyber weapons pose different kinds of collateral damage challenges. In the case of drones, there is no doubt where the strike will occur; the only question is whether civilians in the area may also be killed. In the case of cyber attacks, the question is whether the weapon can be contained days, weeks, or months after its launch. It does not expire after the first contact with the target, and it may take many forms, and reach many places, that its designers never intended. As the Stuxnet attacks showed, the United States and Israel went to some lengths to prevent collateral damage by having the code expire after a set date. Such efforts can mitigate the damage. But even today, elements of that attack live on, repurposed for different kinds of attacks.

The Secrecy Conundrum

One additional conundrum arises when comparing the drone program to the cyber program—namely, secrecy.

As noted earlier, whatever secrecy surrounded the drone program eroded quickly, and by 2013 the president spoke openly about the limits he wanted to place on the weapon's use. Whether one agrees with those limits—or with the concept of moving more drones to the Pentagon so that missions must be accounted for publicly rather than be hidden by the CIA—the doctrine can now be openly debated.

Not so with cyber capabilities, at least not yet. The Pentagon has published some policy and standards, but all the hard questions—including the conditions under which to use the weapons, as well as the kinds of targets that are considered legitimate—have been avoided in public.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

Clearly, a centrifuge facility is on the list of legitimate targets, and so would be a launch facility. But what about a central bank, given the enormous vulnerability of the United States to financial disruption? And if a central back could be targeted, what purpose would be deemed permissible: to gain private information that could be publicized, to deny service for some time, or to corrupt the integrity of financial data? Each type of attack would carry different implications for the object of the attack and for the international standard that it could set. Would an enemy nation's utility grid be an acceptable target, given the vulnerability of our own grid to counterattack? This question does not arise as often in the context of UAVs, which could take out a power station but not an entire electrical network.

And who gets to retaliate? While many Americans now own drones, they are almost all—thankfully—unarmed. Developing malware has fewer barriers. Does it make sense to keep the current US legal ban on "hacking back"? If so, does this prohibition harm the nation's ability to build robust cyber defenses and create a deterrent? Could other forms of active defense, such as inserting beacons to trace the location of stolen data, be developed that would be less risky?

And when would the government intervene to use its own power? If there was a drone attack on New York City, undoubtedly the Air National Guard would step in to protect the air space. But cyberspace is different. Former defense secretary Ashton Carter said he could imagine a federal response in only about 2 percent of all cyber attacks; given the huge number of cyber attacks that take place daily on government and civilian targets, that percentage seems high. So far, only a handful of publicly known cases have merited any significant federal response.

Sparking the Debate

There is no reason these questions cannot be debated by the American people. From 1945 through the Cold War, almost everything about nuclear weapons was classified top secret or above. Yet the country managed to debate nuclear doctrine in the open, determining a set of rules over when the United States would use them. That debate ended in a very different place than it began. The world gained confidence in the US government's ability to control nuclear weapons because of that debate. And the United States set standards that others now follow.

The public is now having a similar debate about drones, though a vigorous press had to help drag the government to that point. Yet in the cyber arena, similar discussions have only just begun. US Cyber Command has started to discuss publicly, in the most halting way, the issues confronting the use of cyber weapons. The fear of revealing the size and scope of the US investment in cyber capabilities, however, has frozen many of the most important discussions. Sooner or later that debate will be opened up just as it was in the nuclear era and just as it has, more recently, on the issue of drones. Such debates have proved critical in defining the use of state-of-the-art technologies that can be turned into new kinds of weaponry. Such discussions will be vital in the cyber realm.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

Notes

David E. Sanger, a national security correspondent for the *New York Times*, is an adjunct lecturer at the Kennedy School of Government at Harvard University and a senior fellow at the school's Belfer Center for Science and International Affairs. The views expressed in this chapter are his own.

1. The author has written extensively about the involvement of Presidents Bush and Obama in the Olympic Games program. See David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), prologue, ch. 8; and David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012, 1.

2. See David E. Sanger, "A Spymaster Who Saw Cyberattacks as Israel's Best Weapon against Iran," *New York Times*, March 22, 2016. The late Meir Dagan, who was the director of the Mossad and a key player in the Israeli side of Olympic Games, chastised the author for not giving Israel enough credit for its role in the operation.

3. See transcript of Obama's talk. Office of Press Secretary, "Remarks by the President in a Conversation on the Supreme Court Nomination," University of Chicago Law School, April 8, 2016, https://www.whitehouse.gov/the-press-office/2016/04/08/remarks-president-conversation-supreme-court-nomination.

4. Ibid.

5. Susan E. Rice, "The Global Campaign against ISIL—Partnerships, Progress, and the Path Ahead," remarks as prepared for delivery at the US Air Force Academy, Colorado Springs, April 14, 2016, https://www.whitehouse.gov/the-press-office/2016/04/14/remarks-national-security-advisor-susan-e-rice-us-air-force-academy.

6. Both Mr. Obama's and Mr. Work's comments were widely reported in April 2016. For example, see David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, April 24, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0.

7. Charlie Savage, *Power Wars: Inside Obama's Post-9/11 Presidency* (New York: Little, Brown, 2015).

8. Eric Schmitt and David E. Sanger, "Pakistan Shift Could Curtail Drone Strikes," *New York Times*, February 22, 2008.

9. Micah Zenko and Amelia Mae Wolf, "Drones Kill More Civilians Than Pilots Do," *Foreign Policy*, April 25, 2016.

10. Jo Becker and Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will," *New York Times*, May 29, 2012, http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?pagewanted=9&_r=1&hp&adxnnlx=1338289213-gFazCDrgzwY2RtQCER9fGQ&pagewanted=all.

11. See Steve Coll, "The Unblinking Stare," *New Yorker*, November 24, 2014, http://www.newyorker.com/magazine/2014/11/24/unblinking-stare.

12. Adam Entous, Siobhan Gorman, and Julian Barnes, "U.S. Tightens Drone Rules," *Wall Street Journal*, November 4, 2011.

13. Ibid.

14. Office of Press Secretary, "Remarks by the President."

15. David E. Sanger, "Bush Sees 'Urgent Duty' to Pre-empt Attack by Iraq," *New York Times*, October 8, 2002.

16. For further discussion of the US consideration of shooting down a Taepodong missile over the Pacific, see my account in *The Inheritance: The World Obama Confronts and the Challenges to American Power* (New York: Three Rivers Press, 2010), 322–23.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.

17. I discussed the incident, and the difference between preemption and preventive war, in David E. Sanger, "Beating Them to the Prewar," *New York Times*, September 28, 2002.

18. David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *New York Times*, December 19, 2014.

19. The Bowman Avenue Dam hack, allegedly carried out by a group of Iranian hackers, took place in Rye Brook, New York, in March 2013. Authorities alleged that seven Iranian hackers penetrated the computer-guided controls of the dam, which was under repair and offline at the time. The Manhattan US Attorney indicted the hackers in March 2016 for both the dam hack and a series of cyber attacks on major US financial institutions. For more information, please see Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2016, http://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html.

© 2017 Georgetown University Press. All Rights Reserved. This PDF is intended for non-commercial use by individuals. For all other types of re-use, please contact Georgetown University Press at gupress@georgetown.edu.