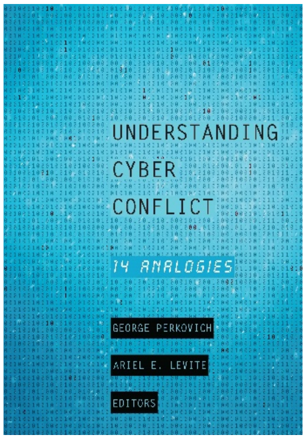
Cyber Weapons and Precision-Guided Munitions

James M. Acton

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



3 Cyber Weapons and Precision-Guided Munitions

JAMES M. ACTON

The development of precision-guided munitions (PGMs)—guided gravity bombs and cruise missiles, in particular—has had profound implications for warfare. Such weapons tend to cause much less collateral damage than their unguided predecessors do, and because they can remain effective when used from a distance, they can also reduce casualties sustained by the attacker. Thus, PGMs have altered national-level decision-making by lowering the political threshold for the use of force and by slowing the likely loss of public support during a sustained military campaign. PGMs have also increased the tactical effectiveness of military operations. They have dramatically improved force exchange ratios (at least against an adversary without these weapons) by reducing the likely number of weapons required to destroy individual targets. In doing so, they have eased logistical requirements and increased the pace at which military operations can be conducted.

Following the 1991 Gulf War, which provided the first high-profile demonstration of the effectiveness PGMs, these weapons were widely seen—both in the United States and abroad—as revolutionary (or, at least, as the technological component of revolutionary military changes).[1] Almost twenty-five years later, a number of analysts have argued that cyber weapons are effecting another revolution in military affairs.[2] This controversial claim is inspired, at least in part, by the analogy between PGMs and cyber weapons.

The similarities between PGMs and sophisticated cyber weapons are striking.[3] Cyber weapons also offer the *potential* of exquisite precision because, if well-designed, they may affect only specific targets and inflict carefully tailored effects.[4] Information technology (IT) is ubiquitous in military operations. As a result, the use of cyberspace for military purposes can confer potential tactical advantages to an attacker, including by further improving force exchange ratios, while placing few, if any, additional demands on the logistical network needed to supply frontline forces. Moreover, the use of cyber weapons involves minimal risk to the lives of the service personnel who "deliver" them and, in general, is likely to cause fewer civilian casualties than even the most carefully designed and executed kinetic attack.[5] As a result, they could further lower the threshold for the use of force. Overall, in fact, states' reasons for wanting cyber weapons are very similar to their reasons for wanting PGMs.

For all the benefits of cyber weapons, they undoubtedly have limitations too. The possibility that cyber weapons can be employed in highly discriminating ways does not imply they must be; like PGMs, cyber weapons can be used in indiscriminate ways. Indeed, many publicly known cyber attacks to date have had distinctly imprecise effects on the target system (for example, by destroying entire computers) and have caused collateral damage against undetermined numbers of other systems and users. That said, there is also reason to suppose that the public record is not representative of cutting-edge cyber capabilities, since more discriminate attacks are easier to hide.

Setting aside the technical and operational challenges of achieving precision in practice, this chapter seeks to exploit the analogy with PGMs to understand some of the other potential limitations of cyber weapons and how militaries might respond to them either by mitigating them or by capitalizing on them. The focus is on three challenges to the effective employment of PGMs and their cyber analogies. The first two challenges—intelligence, surveillance, and reconnaissance (ISR) and battle damage assessment (BDA)—relate to the effectiveness of enabling capabilities. The third challenge is the difficulty of achieving the political objectives for which a war is fought using only standoff attacks.

The Need for Effective Intelligence, Surveillance, and Reconnaissance

An important distinction is drawn in the physical sciences between precision and accuracy. The claim that the population of the United States is 62,571,389 is very precise, but it is not remotely accurate. Similarly, PGMs are almost invariably precise—in the sense that they almost always hit their aim points (or at least very nearby)—but because their intended targets may not always be located at those aim points, PGMs are not always accurate.

To ensure that PGMs are accurate, the location of the intended target must be known both correctly and precisely.[6] The ISR capabilities used to locate targets are, therefore, every bit as important as a weapon's guidance and navigation system. The development of various technologies for acquiring overhead images has made the process of locating stationary, aboveground targets much easier, but it has not guaranteed success. For example, during the bombing of Yugoslavia in 1999, US military planners knew the street address of the Yugoslav Federal Directorate for Supply and Procurement was Bulevar Umetnosti 2.[7] However, because of a combination of human error and out-of-date maps and databases, these planners incorrectly identified the building that corresponded to this address. As a result, although the weapons used in the subsequent strike did indeed hit their intended aim points, they destroyed not a legitimate military target but the Chinese Embassy.

Identifying the location of other types of targets—mobile and underground targets, in particular—is a much tougher problem. The challenge was illustrated during the 1991 Gulf War by the "great Scud hunt," in which Coalition forces attempted to destroy Iraq's Scud missiles and their mobile launchers. Coalition aircraft flew about 1,460 sorties against Scud-related targets—about 215 against the mobile launchers themselves—without scoring a single confirmed kill.[8] The *Gulf War Airpower Survey* attributes the cause of this failure to inadequate ISR and, in particular, "the fundamental sensor limitations of Coalition aircraft."[9] These limitations were compounded by effective Iraqi tactics, such as the use of decoys, which complicated the task of an already inadequate ISR system. Since 1991 significant improvements in ISR (as well as in tactics) have been central to enhancing—at least to some extent—the ability of advanced militaries to destroy dispersed mobile forces, as evidenced by Israel's moderately successful campaign to hunt down Hezbollah's mobile rocket launchers in the 2006 Lebanon War.[10]

Intelligence collection is a similarly important enabling capability for cyber attacks. It contributes to identifying how to penetrate the target IT system, to understanding the system sufficiently well to create a weapon payload with the desired effect, and to ensuring that the payload's effects are limited to the target network.

IT systems are most commonly penetrated as the result of human error. An attacker, for example, might send phishing emails containing a link that, if clicked on, causes malware to be installed. Such attacks are much more likely to be successful if the attacker exploits intelligence about targeted users' names, contacts, and behavioral characteristics—an approach known as "spear phishing." For example, a 2015 report by the cybersecurity firm FireEye details several recent spear-phishing attacks against Southeast Asian governments involved in territorial disputes with China.[11] These attacks appeared to exploit relatively detailed intelligence about targeted users. Much more detailed intelligence can be required to penetrate more sophisticated defenses. For example, to penetrate IT systems at Iran's Natanz enrichment plant, which are surrounded by an air gap, the perpetrators of the Stuxnet attack—believed to be the United States and Israel—reportedly first infected computers belonging to contractors. Personnel employed by these contractors then inadvertently transmitted the virus to Iran's enrichment control system on USB flash drives (other infection strategies were apparently employed too).[12] This approach could have been developed only with detailed knowledge about the organizational structure of Iran's enrichment program. Of course, not all infection strategies rely on user error, but most (if not all) others usually require detailed intelligence about the target, such as knowledge of "zero-day" vulnerabilities—that is, software or hardware flaws that are unpatched because they are unknown to the vendor.

Developing a payload that has the desired effects often requires equally—if not more—detailed intelligence. Stuxnet is a paradigmatic example. The code aimed to destroy Iranian centrifuges by reprogramming the enrichment plant's control system so it altered their rotation speed while simultaneously sending falsely reassuring signals to operators. The development of Stuxnet was reportedly preceded by a huge intelligence-gathering operation on the Natanz facility, which itself relied, at least in part, on cyber espionage.[13] The Stuxnet code was then tested on actual P-1 centrifuges (which are very similar to the IR-1 centrifuges operated by Iran). In one sense, Stuxnet—an exceptionally complicated and sophisticated virus—is something of an extreme example. However, it may well be representative of the challenges associated with developing cyber weapons that can have real-world effects similar to those of extremely precise kinetic weapons.[14] Indeed, that the Stuxnet code also migrated into nontarget machines underscores the practical challenges of achieving precision, while the fact that the code did not activate and thus disrupt the functioning of these machines demonstrates the possibility and importance of sophisticated target reconnaissance and malware engineering.

There are, of course, important differences in intelligence collection for cyber and PGM strikes. Usually, one major purpose of intelligence collection in planning a kinetic strike is to identify the exact location of the target; by contrast, the physical location of an enemy IT system is rarely a concern in planning a cyber attack.

The consequences of intelligence failures are also potentially dissimilar. Poor intelligence about the target of a kinetic attack—as the 1999 bombing of the Chinese Embassy in Belgrade typifies—can lead to high costs in the form of civilian deaths, diplomatic fallout, and reputational damage. For two reasons, the consequences of poor intelligence for a cyber attack are likely to be less significant than for a kinetic attack. First, the distinct chance is that a cyber attack based on poor intelligence will have no effect whatsoever. To be sure, this outcome is not guaranteed; poor intelligence can lead to the cyber equivalent of collateral damage. A 2008 cyber attack by the United States against a terrorist website in Saudi Arabia, for example, is reported to have disrupted more than three hundred other servers because the target IT system was insufficiently understood.[15] However, good programing can presumably minimize the risks of collateral damage, and even if it cannot, collateral damage restricted to cyberspace is likely to be less costly than collateral damage in physical space. Second, cyber attacks are more plausibly deniable than kinetic attacks are. As a result, the reputational cost of launching a cyber attack that causes collateral damage is likely to be less as well.

That said, it is also possible that cyber attacks will be held to a higher standard than kinetic strikes and thus raise the cost of intelligence failures, even if cyber collateral damage is indeed comparatively modest. In fact, precisely because the development of PGMs has changed expectations about what constitutes acceptable collateral damage, advanced states are now held to a much higher standard in assessing whether the application of kinetic force has been proportionate and whether sufficient care has been taken to discriminate between military and civilian targets. Given the potential for cyber weapons to be even "cleaner" than PGMs, cyber operations may be held to a still higher benchmark—at least where they are conducted by states with the capability to develop discriminating weapons.[16]

In any case, there are some interesting analogies about collecting intelligence for cyber operations and for kinetic strikes. One particular challenge of acquiring intelligence for cyber attacks is the inherent mutability of IT systems. For example, security protocols and antivirus software can be improved, zero-day vulnerabilities can be discovered and (usually) patched, software can be updated, and hardware can be replaced. As a result, a cyber weapon cannot remain effective indefinitely, and predicting how long it will remain potent is impossible. In this way, a particularly apt analogy from the physical world is the challenge of gathering intelligence for targeting a mobile asset. Locating a mobile target while it happens to be stationary makes striking it much easier, but given the difficulty of predicting when the target will next move, the window of opportunity for conducting the attack may be of an inherently unpredictable duration.

Given the challenges of targeting mobile assets, many nations have responded to the development of PGMs by increasing the mobility of their military forces (even though mobile systems are almost inevitably more lightly armored than their stationary equivalents and hence easier to destroy if their location is discovered). The analogous approach to cyber defense is to focus resources not only on hardening the IT system—that is, identifying and patching vulnerabilities—but also on regularly modifying an IT system simply for the sake of changing it, a strategy that has been termed "polymorphic cyber defense."[17] This approach attempts to render an attacker's knowledge of the target system obsolete almost as soon as it is obtained. One of the leaders in this field called its technology "Moving Target Defense," making the analogy to the physical world absolutely explicit.[18]

The primary challenge to polymorphic cyber defenses is probably the risk of introducing bugs that could prevent a system from performing as it should. The scale of this risk presumably depends on how much of the system and which parts of it are changed and on the size of the conceptual space of the allowed changes. Thus, there may well be a potential trade-off between greater security and reduced usability. Where states perceive the sweet spot to be may determine the prospects of polymorphic cyber defenses for military applications.

In the physical world, one approach to overcoming the challenge posed by mobility is to reduce the time between detection and engagement. To this end, sensors and weapons have been integrated into the same platform and, in some systems, given the capability to engage autonomously. Israel's Harpy unmanned combat aerial vehicle, for example, is designed to loiter and detect enemy air defense radars (which are frequently mobile) and to attack them automatically.[19] An analogous cyber weapon would have the capability to detect and exploit vulnerabilities autonomously.[20] This author is not qualified to speculate on whether such an "intelligent" cyber weapon could be developed, but the Defense Advanced Research Projects Agency is sponsoring research, including the Grand Cyber Challenge, into cyber defenses that completely autonomously could "identify weaknesses instantly and counter attacks in real time."[21] Such efforts may be dual use: research in detecting cyber vulnerabilities of friendly IT systems and enhancing their defenses could contribute to the development of offensive cyber weapons that can discover enemy IT vulnerabilities.

Beyond mobility, numerous other countermeasures to PGMs have been employed, including air defenses, hardening, deception, interference with navigation and command and control, and human shields. These countermeasures provide fertile ground for further extending the analogy between defenses to PGMs and defenses to cyber weapons (and take it far beyond interference with ISR capabilities), as a few examples demonstrate. Air defenses, which are designed to shoot down incoming PGMs, are analogous to active cyber defenses in which the defender uses its own virus (sometimes known as a white worm) to disable an attacker's. Another countermeasure in kinetic warfare is interfering with the satellite navigation signals, such as those provided by the US Global Positioning System, that many modern PGMs use. Spoofing, for example, involves transmitting fake navigation signals, which are designed to mislead a weapon about its location. Conceptually, spoofing is similar to sinkholing, a form of active cyber defense that involves redirecting data being transmitted by a virus to a computer controlled by the victim of an attack.

An entirely different approach to defending against PGMs (or, indeed, any other form of kinetic attack) is to raise the political costs of a strike. For example, both states and terrorist organizations have used civilians as human shields by hiding weapons in schools, hospitals, and mosques.[22] More prosaically, in every state, many elements of war-supporting infrastructure—including power stations, electricity grids, and oil refineries—are dual use in that they serve both civilian and military purposes. Even if attacking such facilities is legally permissible, it can still be politically costly.

In the cyber world, civilian and military networks also are often one and the same. For example, an overwhelming majority of US military communications data is believed to pass through public networks that also handle civilian data.[23] Going further, organizations that have civilian functions can also conduct offensive cyber operations. For example, China's National Computer Network Emergency Response Technical Team—a body under the Ministry of Industry and Information Technology that is nominally responsible for defending China's civilian networks from attack—may have been involved in offensive cyber operations.[24] This intermingling raises the potential political cost of cyber operations against military targets through the risk of simultaneously implicating civilian assets. The existence of such intermingling inevitably raises the question of whether it is part of a deliberate strategy designed to defend military assets in cyberspace.

The Importance of Effective Battle Damage Assessment

Battle damage assessment is a second enabling capability that is needed to exploit precision to its full extent. Knowledge that a kinetic strike has been successful can avoid wasting resources on unnecessary repeated strikes against the same target. Immediate feedback also enables the attacker to capitalize quickly on the success. For example, if timely confirmation is available that an air defense battery protecting an underground bunker has been destroyed or disabled, mission commanders can exploit the success by authorizing aircraft to attack the bunker before the adversary can take countermeasures (such as evacuation). Conversely, confirmation that the strike against the air defense system was unsuccessful can be used to authorize another attempt to destroy it. The costs of ineffective (or entirely absent) BDA in this scenario could be quite high. If the strike against the air defense system is incorrectly believed to have been successful, the lives of the pilots sent to attack the bunker will be at risk. If the strike was successful but its outcome cannot be confirmed, mission commanders may waste resources on further strikes as well as an opportunity to destroy the bunker.

As a general rule, the more discriminating a strike is, the more difficult BDA becomes. The particular challenges of BDA for PGMs became apparent in the 1991 Gulf War. To give an example, overhead imagery proved relatively ineffective at assessing the effects of attacks on hardened structures. When these attacks were successful, they generally caused extensive internal damage but very little external damage; often the only visible effect of the attack was a hole made by the incoming bomb.[25] Image analysts thus tended to seriously underestimate the effectiveness of strikes against such targets. Thirteen years later, a 2004 report by the US General Accounting Office on the wars in Afghanistan and Iraq highlighted the continued "inability of damage assessment resources to keep up with the pace of modern battlefield operations."[26] The results included the "inefficient use of forces and weapons" and ground advances that were slowed unnecessarily.[27]

In extreme cases, the lack of effective BDA can have truly major consequences. In early 2011 after the US intelligence community acquired evidence of Osama bin Laden's whereabouts, senior American officials debated whether and how to attempt to kill him.[28] Some of President Barack Obama's key advisers reportedly recommended using an aircraft-launched standoff PGM. One of the main reasons—if not the main reason—why Obama rejected this course of action was apparently its lack of any reliable way to verify the strike's success. It could, therefore, have been very difficult to justify the infringement of Pakistani sovereignty, and the United States might have wasted considerable resources in continuing efforts to find bin Laden if he escaped. Obama's decision to use special forces solved the BDA problem but created other extremely serious risks. For example, if Pakistani troops had captured the Americans, the consequences for relations between Washington and Islamabad (not to mention Obama's presidency) would have been much more serious than if a standoff munition had been used.

From a tactical perspective, BDA after a cyber attack is important for many of the same reasons as after a kinetic attack. In fact, such assessments may be even more important because cyber attacks can often produce temporary or reversible effects. Therefore, an attacker may need to discover not just whether the attack achieved the desired effect initially but also whether the target IT system is still compromised and its attack undetected.

The strategic importance of cyber BDA is likely to depend on the particular attack scenario. Because the use of cyber weapons is generally more deniable than the use of kinetic weapons and because cyber attacks may sometimes even go undetected (especially if unsuccessful), states may be less concerned about the need to provide ex post facto justifications for a strike, rendering BDA less important for cyber operations than for kinetic ones. Had some (extremely) hypothetical way to kill bin Laden with a cyber weapon been available, for example, it is conceivable that Obama might have opted for it even without a reliable means of conducting BDA. Using a cyber weapon, however, carries the risk that it might spread and infect third-party, or perhaps even friendly, IT systems. BDA would be extremely important to enable rapid action to mitigate the consequences.

Cyber BDA has been discussed very little in the open literature, so any discussion is necessarily fairly speculative.[29] Nonetheless, governments must have confronted this question. Israel, for example, is reported to have disabled Syrian air defenses with a cyber weapon, in combination with other tools, before its aircraft destroyed Damascus's clandestine plutonium-production reactor in 2007.[30] Given that the human and diplomatic costs of having its aircraft shot down would have been high, Israel presumably had some means of verifying that it had indeed disabled Syria's air defenses.

Network exploitations are presumably the principal tool for cyber BDA. (If a cyber attack has physical effects, other techniques for conducting BDA may be possible. Israel, for example, may have been able to monitor the electromagnetic emissions from Syria's radars.) Indeed, one reason why cyber BDA may be less challenging than physical BDA is that a cyber weapon can potentially be programmed either to conduct an assessment of its own effects or to expropriate information on which such an assessment can be based. By contrast, adding sensors and transmitters for BDA onto a kinetic warhead is extremely difficult, if not impossible.

On balance, however, there are good reasons to expect that cyber BDA is likely to be more challenging than physical BDA, especially for highly precise attacks. (BDA for indiscriminate cyber attacks—against critical infrastructure, say—presents far fewer challenges.) For example, a cyber attack that is designed to prevent an adversary from doing something, such as launching a missile, could present BDA challenges since the attacker might not know whether the cyber weapon had worked until the adversary tried to launch it. More generally, because the effects of many cyber attacks are temporary or reversible, effective BDA cannot rely on a "snapshot" of the target system at a certain moment; instead, continuous monitoring is required. Even if such monitoring is possible, cyber defenses may prevent the information from being sent to the attacker in a timely way. For example, if a cyber weapon is transported across an air gap in a physical storage device, information relevant to BDA could potentially be transported in the same way in the opposite direction; but such a process could be slow and perhaps too slow to be militarily useful. Finally, if using a cyber weapon reveals its own existence, the owner of the targeted IT system can take steps to secure its network and make it less visible, potentially defeating any exploitation being used for BDA. More ambitiously, the owner might even try to fool the attacker by allowing it to exfiltrate deliberately misleading information about the effectiveness of the attack.[31]

Overall, cyber BDA appears to be both important and difficult. Moreover, efforts to defeat BDA perhaps could become a significant feature of cyber warfare. To this author's knowledge, defeating BDA has not been a major focus of states' attempts to undermine advances in PGMs, but efforts to defeat ISR capabilities could have that effect. By contrast, it seems plausible that states could invest significant resources in trying to defeat cyber BDA by developing rapid response capabilities. Indeed, the US military already has in place "Cyber Protection Forces . . . [to] defend priority [Department of Defense] networks and systems," although whether these forces are tasked with attempting to foil adversary BDA attempts is unknown.[32]

Could Cyber Warfare Be Strategic?

Wars are fought for a political purpose. From almost as soon as aircraft were developed, proponents of airpower argued, or hoped, that it would prove to be strategic—that is, have the capability of effecting political objectives by itself. Before the advent of precision-guided weapons, decades of practical experience largely discredited these advocates. Large-scale conventional bombing—including during World War II, the Korean War, and the Vietnam War—may have been called strategic, but this description can be applied accurately only to its scale, not to its effects.[33] To be sure, dumb bombs have been useful military tools on occasion, but with the probable exception of the atomic bombs dropped on Japan in 1945, they never proved decisive.

The development of PGMs has revived belief in the strategic value of standoff attacks—at least if one goes by the actions of technologically advanced states. The United States and its allies have largely relied on air-delivered PGMs and ship- and submarine-launched cruise missiles as their sole or primary military tools in multiple wars: Yugoslavia in 1999, Libya in 2011, and the conflict against the so-called Islamic State that has been waged in Iraq and Syria since 2014. Additionally some senior US military officers expressed hope, both publicly and privately, ahead of the 1991 Gulf War, that the air campaign would force Iraq to withdraw from Kuwait.[34] The tendency to want to count on standoff strikes is not exclusively an American one. Israel's 2006 war in Lebanon and Saudi Arabia's ongoing involvement in the civil war in Yemen also both started as standoff operations, with ground forces deployed only after PGMs proved ineffective at achieving political objectives.

Standoff operations may be extremely attractive to decision makers, but as these examples demonstrate, they have rarely been effective. The bombing of Yugoslavia in 1999 is the one indisputable success, although it was a close-run thing. Seventy-eight days of bombing were required—much more than originally anticipated—by which time the Coalition was close to collapse. Understanding the reasons why standoff strikes with PGMs have failed to achieve their goals casts light on the question of whether cyber weapons could prove to be strategic.[35]

There are two ideal-type strategies by which the employment of PGMs or cyber weapons could effect political change.[36] A *compellence* strategy seeks to inflict pain and demonstrate the willingness to inflict more with the aim of convincing an adversary to concede. A *denial* strategy, by contrast, seeks to weaken the military forces that an enemy is using to prosecute a conflict (and, perhaps, the enemy regime's grip on power). In the real world, these strategies can become indistinct. For example, attacks against a state's military-industrial sector can be justified as denial but may also have, intentionally or otherwise, a punitive effect on civilians. Such attacks are exemplified by both Allied and Axis bombing campaigns in World War II and by much more targeted strikes, such as those against Yugoslavia's electricity and water system in 1999.[37] Conversely, a denial strategy involving strikes against exclusively military targets would administer significant punishment if the adversary's leadership values its own grip on power and its military forces more than it does its citizens' lives and well-being.[38]

Almost by definition, a denial strategy cannot precipitate political change if only standoff weapons—whether kinetic or non-kinetic—are employed. Even if standoff strikes succeed in degrading an adversary's military capabilities, deployed forces are still required to capitalize on this weakness. In 2001, at the start of the Afghanistan war, for example, US airpower played a significant role in weakening Taliban forces, but an armed opposition with broadly equivalent fighting skills to the Taliban was still needed to take and hold territory in physical battles.[39] This opposition force took the form of the Northern Alliance, assisted by US special operations forces. Conversely, Saudi-led airstrikes against Yemen, which began in March 2015, failed to restore President Abdrabbuh Mansour Hadi to power after he had been deposed in a Houthi-led rebellion in large part because he lacked a ground force to take advantage of the strikes. Riyadh apparently hoped that the strikes would spark an anti-Houthi tribal uprising, but it did not occur.[40] As a result, foreign-trained Yemeni fighters were inserted into Yemen in May 2015 and followed by forces from Saudi Arabia and the United Arab Emirates in progressively larger numbers.[41]

Similarly, even if cyber attacks prove highly effective at disrupting an enemy's military operations, physical force will almost certainly be required to exploit this disruption. To be sure, the scenarios in which cyber attacks might prove useful could be very different from the Afghan or Yemeni scenarios since potential adversaries with cyber vulnerabilities range from non-state actors to sophisticated nation-states. But in all cases, success would surely demand a physical force in addition to a cyber force. In fact, against a sophisticated state, such as Russia or China, very considerable physical force might be needed as the state's military would probably remain formidable even after its networks had been compromised—and not least because, in such a conflict, US networks would probably be compromised too.[42]

A second issue is whether cyber weapons could be used to punish an adversary until it submitted. Much of the existing debate on this point revolves around essentially technical questions.[43] How plausible are cyber attacks against critical infrastructure? If such attacks did take place, would they cause large-scale death and long-lasting damage, or would their effects be less costly and more temporary? An even more fundamental question needs to be addressed: Even if cyber attacks against critical infrastructure were relatively easy and even if such attacks caused massive and long-lasting damage, would they actually be effective at compellence?

The history of punitive kinetic attacks demonstrates that, under some circumstances, states (and non-state actors) can withstand astonishing levels of punishment without conceding. To be sure, whether highly damaging cyber attacks were effective at compellence might well depend on what was at stake and the commitment of society at large to the cause. As the bombing of Yugoslavia in 1999 demonstrates, standoff operations can sometimes be effective in forcing one state to bend to another's will. But as the conventional bombing of British, German, and Japanese cities during World War II also illustrates, much greater levels of death and destruction can prove insufficient. Given that cyber weapons are unlikely to inflict costs on anything approaching that scale—even if the direst predictions about their destructive potential are realized—it should not be assumed that they would be effective tools for compellence.

Moreover, compellence may be even more difficult with cyber weapons than with kinetic weapons for at least one reason: compellence does not rely on inflicting pain per se but on the threat to keep doing so until an adversary concedes.[44] Meting out some punishment may well be necessary to make such a threat credible, but inflicting even high levels of pain may not establish credibility if the victim believes that the attacker is unwilling or unable to continue. This theoretical problem could become a real complication in a campaign of cyber compellence since, after the first wave of attacks, the victim might be able to take steps that would make further attacks much more difficult. Most obviously, the victim could analyze the virus (or viruses) that perpetrated the attacks and the means by which its IT systems were penetrated and use this information to patch vulnerabilities. Next, it could implement enhanced cybersecurity measures to reduce generic vulnerabilities, and it could try to "hack back" against the perpetrator to disrupt further attacks. Such steps would reduce the likelihood of compellence being successful. Again, however, there could be no guarantees. The time required to analyze the cyber weapon could be too long for the results to be useful in preventing further attacks.[45] Even if the analysis could be completed quickly, its utility might be limited if the attacker had developed multiple cyber weapons that all worked in different ways. Nonetheless, the basic point remains: compared to kinetic compellence, cyber compellence faces additional challenges.

To be sure, steps to enhance the cybersecurity of critical infrastructure are highly worthwhile. Although the repeated unsuccessful attempts at compellence with kinetic weapons suggest that cyber compellence might also prove unsuccessful, it still might be attempted. Meanwhile, some actors, including terrorists, may try to attack critical infrastructure for reasons other than compellence. Nonetheless, understanding the challenges of cyber compellence is useful in constructing more effective cyber defenses. Specifically, rapid response capabilities that enable a state to analyze cyber attacks on critical infrastructure quickly and use that information to prevent further attacks would be particularly useful in defeating attempts at compellence. Indeed, the US Department of Defense has recently stood up "National Mission Forces . . . [to] defend the United States and its interests against cyberattacks of significant consequence."[46] While the exact task of these forces is not publicly known, simply their existence might contribute to deterring attempts at compellence.

* * *

Focusing on the analogy between cyber weapons and PGMs risks giving the incorrect impression that the former are simply a new kind of the latter. They are not; further, they have many important differences, both obvious and subtle. Cyber weapons can often reach their targets effectively and instantaneously, though they can also be designed to have a delayed effect. Kinetic weapons generally travel much more slowly than cyber weapons, but if and when the former reach their targets, they usually have an almost instantaneous effect. PGMs are also limited by range, a concept without much meaning in cyberspace. Some cyber weapons can create reversible effects, whereas the effects of kinetic weapons are almost always irreversible.

More subtly, cyber vulnerabilities can usually be addressed relatively quickly. Thus, it is unlikely that a cyber weapon can be used repeatedly over the course of a multiday conflict without becoming obsolete. In fact, a cyber weapon might be effective only once. As a result, even if a state has stockpiled many different cyber weapons, it likely will face strong pressures to be highly selective in their employment. By contrast, while using a kinetic weapon certainly can provide an adversary with information that is useful in developing countermeasures, exploiting such information generally takes much longer than in the case of cyber weapons (the development of a new air defense system, for example, typically takes years). Therefore, advanced states can and do stockpile PGMs of a given type in large quantities and are increasingly using such weapons by default instead of dumb bombs. Indeed, as conflicts proceed, states tend to use ostensibly precise weapons in increasingly less selective ways, vitiating the putative special purpose of these weapons and depleting their stocks.

Another potential false impression is that based on the experience of PGMs, cyber weapons are unlikely to have significant implications for warfare. While it is still far too early to assess with any confidence exactly how military operations in cyberspace will change armed conflict, that such changes will be far-reaching seems entirely possible. Indeed, for all the limitations associated with PGMs, plenty of evidence shows that their development does represent a revolution in military affairs. These weapons are not usually able to achieve war aims by themselves, but they have altered leaders' calculations about the use of force and have thus altered national strategies. Moreover, because of the challenges associated with the effective employment of PGMs, the precision revolution is still incomplete. As states further develop ISR and BDA capabilities (and overcome other barriers), PGMs can be expected to become more potent at the tactical level and perhaps even at the strategic level too.

Similarly, the advent of cyber warfare will probably further lower the threshold for the use of force. Senior officials—at least in the United States—have said as much. In 2014, for example, Eric Rosenbach, then an assistant secretary of defense, stated, "The place where I think [cyber operations] will be most helpful to senior policymakers is what I call in 'the space between.' What is the space between? . . . You have diplomacy, economic sanctions . . . and then you have military action. In between there's this space, right? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest."[47]

Yet the analogy with PGMs suggests that the ability of states to employ cyber weapons effectively is likely to lag their desire to use them. In fact, it may take decades not only for states to understand the limitations of cyber weapons and whether and how these limitations can be overcome but also for the full implications of cyber warfare to become apparent.

Notes

1. For example, Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest* 37 (Fall 1994): 30–42.

2. For example, Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 18, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-4/Nye.pdf; and Kenneth Geers, *Strategic Cyber Security* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, June 2011), 112, https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF.

3. This comparison has been discussed in, for example, Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (Spring 2014): 85–87, https://www.usnwc.edu/getattachment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx; and Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), 7–12, http://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf.

4. For the purposes of this chapter, a *cyber weapon* is defined as a computer program designed to compromise the integrity or availability of data in an enemy's IT system for military purposes, and a *cyber attack* is defined as the use of a cyber weapon for offensive purposes. A cyber weapon may be used by itself or in concert with other weapons (kinetic or otherwise). Its effects may be felt purely in cyberspace or in physical space too. Cyber exploitation that compromises only the confidentiality of data is not considered a form of cyber attack.

5. Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, October 19, 2011, http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/.

6. In technical jargon, the target location error should not be significantly larger than the weapon's circular error probable.

7. George Tenet, "DCI Statement on the Belgrade Chinese Embassy Bombing," testimony to the Permanent Select Committee on Intelligence of the US House of Representatives, July 22, 1999, https://www.cia.gov/news-information/speeches-testimony/1999/dci_speech_072299.html.

8. Barry D. Watts and Thomas A. Keaney, "Effects and Effectiveness," in *Gulf War Air Power Survey*, vol. 2 (Washington, DC: US Government Printing Office, 1993), pt. 2, 331–32, http://www.dtic.mil/dtic/tr/fulltext/u2/a279742.pdf.

9. Ibid., 340.

10. Uzi Rubin, *The Rocket Campaign against Israel during the 2006 Lebanon War*, Mideast Security and Policy Studies 71 (Ramat Gan: The Begin-Sadat Center for Strategic Studies, Bar-Ilan University, June 2007), 19–21, https://besacenter.org/mideast-security-and-policy-studies/the-rocket-campaign-against-israel-during-the-2006-lebanon-war-2–2/.

11. FireEye and Singtel, *Southeast Asia: An Evolving Cyber Threat Landscape*, FireEye Threat Intelligence (Milpitas, CA: FireEye, March 2015), 13, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf. In one attack, for example, one state's air force was targeted with "spear-phishing emails that referenced the country's military and regional maritime disputes . . . [and that] were designed to appear to originate from email accounts associated with other elements of the military." The report implies—but does not state explicitly—that China was responsible for the attacks.

12. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 337–41; and Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Version 1.4 (Cupertino, CA: Symantec Security Response, February 2011), especially 7–11, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

13. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

14. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities* (Washington, DC: National Academies Press, 2009), 118; and Krepinevich, *Cyber Warfare*, 43–44.

15. Ellen Nakashima, "U.S. Eyes Preemptive Cyber-Defense Strategy," *Washington Post,* August 29, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803312.html.

16. One worrying possibility is that nations with fewer resources will focus on simpler, less discriminating cyber weapons that contain fewer safeguards against their spread. Not only are such weapons likely to cause much more collateral damage than more sophisticated cyber weapons would but also, unlike with PGMs, such damage might be felt far from the physical location of the target.

17. Dudu Mimran, "The Emergence of Polymorphic Cyber Defense," dudumimran.com (blog), February 10, 2015, http://www.dudumimran.com/2015/02/the-emergence-of-polymorphic-cyber-defense.html.

18. Morphisec, "What We Do," http://www.morphisec.com/what-we-do/. Interestingly, this technology is designed to "fit around" existing Windows-based operating systems.

19. "IAI Harpy," *Jane's Unmanned Aerial Vehicles and Targets*, September 30, 2015, www.ihs.com.

20. Existing cyber weapons may be able to execute preplanned attacks autonomously, but that is a much less stressing task.

21. Defense Advanced Research Projects Agency (DARPA), "Seven Teams Hack Their Way to the 2016 DARPA Cyber Grand Challenge Final Competition," July 8, 2015, http://www.darpa.mil/news-events/2015–07–08.

22. For example, Terrence McCoy, "Why Hamas Stores Its Weapons inside Hospitals, Mosques and Schools," *Washington Post*, July 31, 2014, https://www.washingtonpost.com/news/morning-mix/wp/2014/07/31/why-hamas-stores-its-weapons-inside-hospitals-mosques-and-schools/.

23. Michael Gervais, “Cyber Attacks and the Law of War,” *Journal of Law & Cyber Warfare* 1, no. 1 (Winter 2012): 78–79.

24. Bill Marczak et al., “China’s Great Canon,” Research Brief (The Citizen Lab and Munk School of Global Affairs, University of Toronto, April 2015), 11, https://citizenlab.org/wp-content/uploads/2009/10/ChinasGreatCannon.pdf.

25. Watts and Keaney, “Effects and Effectiveness,” 30–47.

26. US General Accounting Office, *Military Operations: Recent Campaigns Benefited from Improved Communications and Technology, but Barriers to Continued Progress Remain*, GAO-54–547 (Washington, DC: General Accounting Office, June 2004), 24, http://www.gao.gov/new.items/d04547.pdf.

27. Ibid, 23–24.

28. Mark Bowden, “The Hunt for ‘Geronimo,’” *Vanity Fair*, October 12, 2012, http://www.vanityfair.com/news/politics/2012/11/inside-osama-bin-laden-assassination-plot.

29. For rare examples, see Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 87–90; and Maj. Richard A. Martino, “Leveraging Traditional Battle Damage Assessment Procedures to Measure Effects from a Computer Network Attack” (graduate research project, Air Force Institute of Technology, Air University, June 2011), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA544644. Much of the available literature on BDA focuses on defensive BDA, or a victim’s assessment of the effects of a cyber attack on its own networks. This task is easier than an offensive BDA since the attacker has no guarantee of being able to maintain access to the victim’s networks.

30. David A. Fulghum, Robert Wall, and Amy Butler, “Cyber-Combat’s First Shot: Israel Shows Electronic Prowess: Attack on Syria Shows Israel Is Master of the High-Tech Battle,” *Aviation Week & Space Technology* 167, no. 21 (November 26, 2007): 28–31.

31. Libicki, *Conquest in Cyberspace*, 88–90.

32. US Department of Defense, “The Department of Defense Cyber Strategy” (Washington, DC: Department of Defense, April 2015), 6, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

33. See, for example, Richard Overy, *The Bombers and the Bombed: Allied Air War over Europe, 1940–1945* (New York: Viking, 2014).

34. Watts and Keaney, “Effects and Effectiveness,” 15, 341, 378.

35. For the explicit or, through analogy with nuclear weapons, implicit case that cyber weapons are strategic, see, for example, Geers, *Strategic Cyber Security*, 15; and Mike McConnell, “Mike McConnell on How to Win the Cyber-War We’re Losing,” *Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. For similar claims in the Russian and Chinese military literature, see Krepinevich, *Cyber Warfare*, 3–4.

36. For a classic theoretical discussion, see Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca: Cornell University Press, 1996), ch. 2.

37. Philip Bennett and Steve Coll, “NATO Warplanes Jolt Yugoslav Power Grid,” *Washington Post*, May 25, 1999, https://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/belgrade052599.htm.

38. Within the nuclear deterrence literature, the term “aspects of state power” has been used to describe what dictatorial regimes are hypothesized to value. Michael Quinlan, *Thinking about Nuclear Weapons: Principles, Problems, Prospects* (Oxford: Oxford University Press, 2009), 126.

39. Stephen D. Biddle, “Allies, Airpower, and Modern Warfare: The Afghan Model in Afghanistan and Iraq,” *International Security* 30, no. 3 (Winter 2005/2006): 161–76.

40. David B. Ottaway, “Saudi Arabia’s Yemen War Unravels,” *The National Interest*, May 11, 2015, http://nationalinterest.org/feature/saudi-arabias-yemen-war-unravels-12853.

41. Michael Knights and Alexandre Mello, “The Saudi-UAE War Effort in Yemen (Part 1): Operation Golden Arrow in Aden,” Policywatch 2464 (Washington, DC: Washington Institute for Near East Policy, August 10, 2015), http://www.washingtoninstitute.org/policy-analysis/view/the-saudi-uae-war-effort-in-yemen-part-1-operation-golden-arrow-in-aden.

42. The question of how militaries would fare without their IT systems is discussed in Martin C. Libicki, “Why Cyber War Will Not and Should Not Have Its Grand Strategist,” *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 29–30, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA602105.

43. For various different perspectives in this debate, see Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (July 2013): esp. 385–97, 402–4; Krepinevich, *Cyber Warfare*, 39–65; and Richard A. Clarke and Robert K. Knake, *Cyber War: The Next National Security Threat and What to Do about It* (New York: HarperCollins, 2010), 64–68, 96–101.

44. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 70.

45. The attacker could also try to issue a compellent threat before using cyber weapons. However, making a credible threat not only is difficult but also would alert the victim to the (possible) presence of a cyber weapon in its IT systems. Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security* 38, no. 2 (Fall 2013): 59.

46. US Department of Defense, *Department of Defense Cyber Strategy*, 6.

47. Quoted in Tim Maurer, “The Future of War: Cyber Is Expanding the Clausewitzian Spectrum of Conflict,” *Foreign Policy*, November 13, 2014, http://foreignpolicy.com/2014/11/13/the-future-of-war-cyber-is-expanding-the-clausewitzian-spectrum-of-conflict/.