2 Nonlethal Weapons and Cyber Capabilities

LT. GEN. ROBERT E. SCHMIDLE JR. (USMC, RET.), MICHAEL SULMEYER, AND BEN BUCHANAN

Scholars have considered many analogies for cyber capabilities, grappling with how these capabilities may shape the future of conflict.[1] One recurring theme in this literature is the comparison of cyber capabilities to powerful, strategic capabilities with the potential to cause significant death and destruction.[2] This theme is understandable. Reports of malware that can penetrate air-gapped networks and cause physical effects can easily stimulate worst-case thinking. Moreover, relative silence from senior government leaders about cyber capabilities can fuel speculation that nations are amassing devastating arsenals of malware.[3] Increasing connectivity from consumer products to critical infrastructure control systems creates the prospect of widespread vulnerability across societies.[4] Analogies to different methods of state-to-state coercion are therefore quite common.

However, no one has ever been killed by a cyber capability. With this in mind, perhaps another set of analogies for cyber capabilities—not destructive, strategic capabilities but those that are nonlethal—should be considered. The US Department of Defense for decades has developed a range of nonlethal weapons for its forces, yet to our knowledge, scant academic work to date has considered how nonlethal weapons might provide some additional conceptual insight into cyber capabilities.

In this chapter, we examine nonlethal weapons and cyber capabilities and suggest that for conceptual purposes it may be useful to analogize between them across four areas: their ability to incapacitate, the reduced collateral damage they inflict, the reversibility of their effects, and their ability to deter. In so doing, we show the usefulness and the limits of analogizing cyber capabilities to nonlethal weapons. Ultimately, we conclude that these four areas of convergence between nonlethal weapons and cyber capabilities make for a novel conceptual analogy that would serve policymakers well as they consider future employment of cyber capabilities.

In our conclusion, however, we highlight one important limitation of this approach: Department of Defense leaders have faced difficulty in gaining approval to use nonlethal capabilities. We briefly explore reasons why nonlethal weapons have so seldom been authorized and offer some observations as to why cyber capabilities may be easier to employ in the future. We base this distinction

© 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.

on the fact that most nonlethal weapons target opposing personnel, whereas most cyber capabilities target opposing matériel.

Before commencing our analysis, we offer one preliminary note about terminology. Already we have noted that we examine cyberspace "capabilities" as opposed to cyber "weapons." The distinction is not pedantic. When we write of nonlethal "weapons," the intent of these tools is in clearer focus—to inflict bodily harm or physical damage.[5] However, the cyber tools discussed in this chapter are not always weaponized *ex ante*. Instead, they offer certain capabilities: some that may be used offensively, some in self-defense, and still others for penetration testing. Because code is not inherently weaponized, we use the term "capabilities" to cover the full of range of what technologies in cyberspace have to offer.

Characteristics of Nonlethal Weapons

To more fully understand the proposed analogy between nonlethal weapons and cyber capabilities, we must first understand the basics of nonlethal weapons. The Department of Defense defines *nonlethal weapons* as "weapons, devices, and munitions that are explicitly designed and primarily employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the target area or environment."[6] Cyber capabilities are excluded from this definition. Nonlethal weapons can provide operating forces with options to de-escalate situations, minimize casualties, and reduce collateral damage. By providing commanders with these additional options, nonlethal capabilities can be of unique value, sometimes proving to be more appropriate than their lethal counterparts.

Nonlethal weapons are often divided into two categories depending on their direct target. First, many nonlethal weapons are identified as serving a "counter-personnel" role because they target the human body itself. A notable example is oleoresin capsicum spray, which is more commonly known as pepper spray. When sprayed at a target, the chemical compounds in the spray act as an irritant to the eyes, causing tears, pain, and temporary blindness. This effect makes it more difficult for the target to engage in combat or other threatening activities.

The second category of nonlethal weapons targets machines, not people. An example of this sort of capability is the so-called spike strip. Derived from the older caltrop—which was used as a counter-personnel, counter-animal, and counter-vehicle weapon—the spike strip comprises long, upward-facing metal barbs linked together in a long chain. Each barb is sufficient to puncture the tires of many vehicles; so, when laid across a roadway, the spike strip can slow or stop vehicle movement until the tires have been replaced. Many spike strips are designed to gradually let the air out of affected vehicles' tires, minimizing the harm done to passengers and reducing the risk of collateral damage.

Across both counter-personnel and counter-machine nonlethal weapons, four characteristics are evident. First, their primary purpose is to incapacitate their targets. Second, they do so with minimal collateral damage, and, third, in a way that is often temporary or reversible. Finally, nonlethal weapons can serve

© 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.

as a limited deterrent in tactical situations. These characteristics are key points of comparison in making the analogy to cyber capabilities.

Operational History of US Nonlethal Weapons

One can trace the origins of nonlethal weapons in warfare to the development of modern chemistry, which began in the eighteenth century. By the mid-nineteenth century, consideration was given to using chemical weapons in the Crimean and US Civil Wars.[7] To be sure, chemical weapons would eventually become quite deadly, but initially the intent behind their use was not to kill but to force the enemy to disperse. Militaries apparently did not embrace using chemicals in warfare until World War I, when the German army launched the first chemical weapons attack on April 22, 1915, near Ypres.[8] As the United States entered the war, it institutionalized its chemical munitions research and development into a Chemical Warfare Service with the US Army.[9] Among the chemical weapons developed during the war, multiple armies used tear gas, which remains a nonlethal weapon in today's law enforcement and military arsenals.[10]

At the war's conclusion, the US Army rapidly demobilized its chemical weapons corps and seemed poised to all but abandon research into this class of weaponry.[11] The army's experts secured employment in civilian jobs, and surplus material was either sold or transferred to other parts of the government.[12] Thus concluded the US Army's initial efforts to explore how gas could be used as a chemical, nonlethal weapon.[13] Thereafter, the 1925 Geneva Protocol prohibited the use of chemical weapons in war.[14]

Even without this protocol, it seems unlikely that tear gas–related chemical agents would have been as effective in World War II, at least in the European theater. The rise and increasing adoption of motorized and mechanized forces neutralized the utility of chemical agents to disperse forces from fixed positions.[15] However, militaries used smoke as a tactical, nonlethal enabler during World War II, often to obscure their own positions rather than to force the enemy to reposition.[16] Variants included white phosphorus, smoke pots, oil smoke generators, aircraft-delivered smoke tanks, and even colored smoke munitions for signaling.[17]

Development of chemical agents continued after World War II. The use of herbicides and other agents during the Vietnam War, while not deemed to violate the 1925 Geneva Protocol, proved to be sufficiently controversial and damaging that President Gerald Ford issued an executive order renouncing the first use of herbicides and riot control agents in war.[18]

Other technologies emerged that offered militaries options between "don't shoot" and "shoot to kill." The United Kingdom used rubber and plastic bullets in Northern Ireland in the 1970s. Indeed, by one account the British military fired 55,834 rubber bullets between 1970 and 1975.[19] During Desert Storm, the United States fired cruise missiles filled with carbon fiber that disrupted Iraq's power stations.[20] In March 1991 Secretary of Defense Dick Cheney asked his lieutenants

© 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.

Paul Wolfowitz and Zalmay Khalilzad to lead a Non-Lethal Warfare Study, but it is unclear what, if anything, came of this examination.[21]

Just how useful nonlethal weapons could be was perhaps most clearly demonstrated during the US Marine Corps' presence in Somalia in the mid-1990s. Their commander, Lt. Gen. Anthony Zinni, in a 1994 hearing spoke of the virtues of nonlethal weapons. "Non-traditional operations," he said, "often involve police-like actions that would be best dealt with by non-lethal means. Crowd control, demonstrations, petty theft, acts of urban violence in populated areas, are examples of situations that could best be handled all or in part by non-lethal weapons. . . . These non-lethal means also permit forces to demonstrate resolve or provide a show-of-force without endangering lives."[22]

A year later, Zinni's Marines provided cover when several thousand United Nations (UN) forces withdrew from Somalia. The former had trained to use a variety of nonlethal weapons, including pepper spray, flash bangs, and road spikes.[23] To control hostile crowds, they were equipped with foam guns and sticky guns, as well as hard sponge projectiles.[24] The Marines also warned the local populace that they possessed these nonlethal weapons. Ultimately, the mission to secure the extraction of the UN forces was successful. No Marines were killed.[25] Zinni noted afterward, "Our experience in Somalia with non-lethal weapons offered ample testimony to the tremendous flexibility they offer to warriors on the field of battle."[26]

Later in the 1990s, the Defense Department attempted to institutionalize research and development for a broader array of nonlethal weapons.[27] Yet few capabilities were available to support US forces after they invaded and occupied Iraq in 2003. A 2004 Council on Foreign Relations task force on nonlethal weapons found that these weapons "could have helped to reduce the damage done by widespread looting and sabotage."[28] Its report was one of the last major studies of the US military's use of nonlethal weapons. There is little evidence that prioritization or resources have changed since then.

With this history of experimentation but not integration in mind, we return to the analysis of how four qualities of nonlethal weapons, especially those that are counter-matériel, make for a conceptually useful analogy to cyber capabilities.

Incapacitation

Nonlethal weapons incapacitate their targets by attacking critical parts of the targeted machine, such as tires on a vehicle, and disabling them. Cyber attacks can work in the same way, attacking critical parts of a computer system and either overwhelming them or disabling them. Information security professionals have long argued that a cyber operation can do harm in one of three ways.[29] First, it can target the confidentiality of data in a computer system, stealing sensitive data and perhaps making it public. Second, it can target the integrity of a computer system by inputting malicious commands that adversely (and clandestinely) affect its functionality or by corrupting important data. Third, it

© 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.

can target the availability of a computer system, disabling access to it at a critical time.

An example of the incapacitation function is the cyber operation that accompanied the purported Israeli air strike on Syria in 2007. The cyber operation corrupted the integrity of the Syrian air defenses. While operators of the Syrian air defense system believed their radar was functional and that it presented them with an accurate display of the area, in fact the radar systems did not show the Israeli jets entering Syrian airspace.[30]

A more common example of incapacitation via cyber operation is known as a *denial of service* attack, which targets the availability of important computer services by overwhelming them with data. An ocean of incoming data prevents the targeted systems from responding to legitimate requests. Finally, some capabilities achieve an incapacitating effect by targeting both the integrity and the availability of a target. For example, the 2014 attack on the Sands Casino in Las Vegas targeted the integrity of critical computer code and adversely impacted the availability of the overall system. When this critical code was erased or corrupted, the affected computers did not function.[31]

By definition, cyber capabilities target machines. As a result, it is more difficult, but not impossible, to imagine a cyber capability that is directly counter-personnel. One possible lethal capability is code that manipulates a vital medical device, such as a pacemaker. Indeed, in 2007 Vice President Cheney had the wireless functionality on his pacemaker disabled out of fear that it could be attacked.[32] More broadly, weaknesses in the Internet of things could allow malicious code to incapacitate critical devices at critical times, leading to the possibility of targeted attacks with a direct effect on personnel.[33] Even if cyber capabilities are not lethal now, if these sorts of attacks become more achievable, they might be more lethal in the future as well.

Whether an attack has lethal effects or not, electronic systems targeted by cyber capabilities might in some instances be so important to an individual that incapacitating the system could have debilitating counter-personnel effects. For example, targeting cellular phone networks or other communications systems can affect an individual's ability to coordinate illegal, hostile, or otherwise dangerous behavior. It could also perhaps be argued that targeting confidential systems, such as the theft of data from personnel databases, has an effect on personnel and could be used for blackmail. In this last case, however, the delay between operation and effect is substantially longer than is the case for most nonlethal weapons. Thus, on the matter of incapacitation, the analogy is strongest between counter-matériel nonlethal weapons and cyber capabilities that attack the integrity and availability of targeted systems.

Minimization of Collateral Damage

Similar to nonlethal weapons, some cyber capabilities can be deployed to minimize collateral damage. When it comes to malicious computer code, this sort of minimization can take one or both of two forms—first, preventing the spread of

© 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.

computer code beyond the target and, second, minimizing the harm the code causes to nontarget systems if it does in fact spread.

On the first point, intermediate systems are commonly breached in a cyber operation as stepping-stones to reach the target. This is especially true if direct access to the target is denied. For example, as a means of getting malicious code into a facility that is not connected to the Internet and is thus harder for an attacker to access, the authors of Stuxnet reportedly targeted a number of Iranian contractors who were servicing the country's nuclear program.[34] But such intermediate infections can be difficult to control in cases where the capability's propagation mechanism, or the code it uses to spread from machine to machine, is automatic. In the Stuxnet case, the code spread beyond the original authors' intent, reaching other systems and eventually coming to the attention of the information security community.[35]

Second, authors of malicious code have shown some capability to minimize the harm such code can do, even if it spreads. For example, the authors of Stuxnet, Gauss, and other malicious code placed targeting guidance in the code.[36] This targeting guidance prevented the code from launching its most significant and damaging payloads unless the malware arrived at the correct target. While reports indicate these mechanisms were not perfect at preventing all ill effects, they automatically and substantially constrained the damage done by the malicious code once it spread.[37] It is worth noting, however, that adding such constraints requires a great deal of information about the particulars of the target system, information that will likely need time and previous operations to collect.[38]

Another important area of overlap between nonlethal weapons and cyber capabilities is related to minimizing collateral damage. Policy guidance offered by the US Defense Department does not prioritize cyber capabilities or nonlethal weapons over potentially more destructive kinetic ones. While cyber capabilities, at some point in the future, might offer a commander the ability to achieve military-relevant effects with only a minimal risk for collateral damage or loss of life, the complexity of computer networks at present greatly complicates the confidence a commander can have in the ability to achieve precise effects exactly when desired. Battle damage assessment is subject to similar limitations. In some instances, therefore, a commander would reasonably prefer non-cyber capabilities over a vast arsenal of cyber capabilities if the former could give greater odds for the success of an operation.

Based on these examples, given enough effort, time, and operator ability, sophisticated cyber capabilities present some prospects for minimizing collateral damage to systems besides the target. However, it is hard to generalize this point and argue that this central characteristic of nonlethal weapons can be a characteristic of all cyber capabilities. In addition, failures to prevent collateral damage do occur. Especially with capabilities as new and complex as cyber ones, the unintended consequences of particular capabilities may cause additional or unexpected damage. On the matter of collateral damage, then, the analogy is as much aspirational as operational. Some cyber capabilities are narrowly targeted

© 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.

and may be wielded carefully by sophisticated actors, but certainly not all of them are.

Reversibility

The analogy functions similarly when it comes to reversibility, for some cyber capabilities, but not all, are reversible. We identify four categories of reversibility: capabilities that are not reversible; capabilities that are reversible after some reasonably constant period of time, depending on environmental conditions; capabilities that are reversible at the discretion of the operator; and capabilities and their effects that could be reversible by the target but require some time, material, or effort to do so.

Various nonlethal weapons fall into each of the four categories. For example, in the first category, some kinds of nonlethal munitions do harm to the body that, though not fatal, cannot be undone; however, they are comparatively rare. For example, a rubber bullet could possibly cause some harm to the body that is not easily undone. In the second category, flash bang grenades and tear gas cause paralysis for a time, but their effects eventually dissipate. In the third category, operators can turn on and off electronic jamming, lasers, or sonic capabilities. And in the last category, the spike strips discussed earlier require the target to acquire new tires.

Cyber capabilities exist in three of the four categories. In the first category, some sabotage attacks are difficult to reverse easily, especially if they destroy critical material or data. Stuxnet is an example, though it was substantially more destructive than nonlethal weapons are. We do not know of any cyber capabilities that fall into the second category, which sees effects dissipate over time, depending on environmental conditions.

Other cyber capabilities, such as ransomware, fall into the third category because they paralyze systems until an operator directs otherwise. When ransomware affects a system's capability, important data is encrypted in such a way that the legitimate user cannot access it until the criminal operating the ransomware decrypts it—usually for a fee. Capabilities that have an intentionally intermittent or time-bound effect would also fall into this third category. Still other cyber capabilities, such as some wiping operations, are best placed in the fourth category, as the target may be able programmatically to reverse it but would require a substantial amount of effort or time to do so. For example, a target might possibly recover data from "wiped" hard drives, depending on how the wiping attack was done, but it is beyond the capabilities of most ordinary users.

It is worth noting that some capabilities exist in both the third and fourth categories. For example, denial of service attacks—which overwhelm a target with meaningless data—can be not only turned off by an operator but also thwarted by the target's taking certain countermeasures.

From this analysis, we conclude that the qualities of reversibility that are most often intended when using nonlethal weapons are often similar to the most

© 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.

frequent kinds of cyber capabilities employed today. With some rare but important exceptions, such as attacks that destroy physical infrastructure, the damage caused by even some data-destroying cyber capabilities is often reversible in that computers and systems can be repaired with sufficient time and resources. However, as a practical matter, most victims of such attacks may find replacing rather than repairing their malfunctioning systems is more prudent. Given that the majority of contemporary compromises of confidentiality, integrity, and availability of data are perpetrated through reversible means (like denial of service), we feel the analogy to nonlethal weapons has value in this area of analysis.

Deterrence

Analogizing nonlethal weapons and cyber capabilities in the area of deterrence is possible but not as straightforward as the preceding three areas of analysis. Deterrence is an important but reasonably narrow concept when it comes to nonlethal weapons. For cyber capabilities, questions of deterrence are more complex, as applications converge with and diverge from the concept's use in nonlethal weapons. Much has been written about deterrence of cyber capabilities as well as about using these capabilities for deterrence; thus, we briefly provide an outline of the underpinning of deterrence and examine how the analogy applies.[39]

When considering deterrence, the initial questions to consider are, whom do we wish to deter from doing what, and what would we like them do to instead? Any discussion about deterrence must be tailored around this "deter whom from doing what" foundation. During the Cold War, the term "nuclear deterrence" was often shorthand for "deterring the Soviet Union from launching a nuclear-armed attack."[40] But this case of deterrence can obscure the fact that other kinds of deterrence exist. While the Cold War case mostly involved deterrence of a specific actor, some deterrents are general and apply to large groups of actors.

Similarly, while nuclear deterrence is absolute—that is, seeking to stop any use of an atomic weapon—other deterrents are restrictive and seek to minimize the effects and occurrence of an unwanted activity as much as possible while acknowledging implicitly that some will occur.[41] Deterring crime is an example that is both general and restrictive: police do not always know which individual in society is a would-be criminal, and they also recognize that despite measures to deter its occurrence, some amount of crime is inevitable.

The two traditional methods of deterrence are cost imposition and denial.[42] Deterrence by *cost imposition* operates via a (tacit or explicit) credible threat of retaliation to such a degree that the attacking state would find commencing the unwanted activity prohibitively costly. Deterrence by *denial* operates by convincing an adversary that even if it does not fear cost imposition, the benefits it seeks will be checked due to effective defenses. Together the two can make certain actions unappealing. Deterrence by denial can reduce the chances of success, while fear of retaliation can make certain actions prohibitively costly.

Nonlethal weapons can function, depending on the capability, as deterrents by denial or by threatening cost imposition. Many counter-matériel and counter-

© 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.

personnel capabilities impose comparatively minimal costs on an adversary but can reduce or deny the adversary's capability to carry out an unwanted action.

A tactical example from Somalia demonstrates that nonlethal lasers functioned as a means of threatening total retaliation, signaling to potential adversaries that they had been identified and would be neutralized if they attacked US forces. That is, a laser beam shined on a target warned that a bullet could follow.

Some cyber capabilities also can work as deterrents by denial or deterrents by cost imposition, depending on the capability. China's Great Firewall is an example of deterrence by denial. The system, which actively intercepts unwanted Internet activity in Chinese networks and prevents it from connecting to blocked servers, aims not only to prevent but also to deter actions that the Chinese government deems undesirable. It is a scalable and general deterrent across the broader population rather than a narrowly crafted one for a small group of actors. Still, it is restrictive rather than absolute, as the Chinese surely know that some individuals find their way around the firewall.

China's so-called Great Cannon is an example of deterrence by cost imposition. In 2015 members of the popular code repository and software development site GitHub, to which anyone can upload code or text, began uploading *New York Times* articles and other content the Chinese viewed as subversive. In response, while leveraging their position of privilege on the Chinese Internet that is made possible by the Great Firewall, Chinese actors launched a massive denial of service attack and took GitHub offline for a time. By imposing costs on GitHub, the Chinese carried out a form of deterrence by cost imposition to GitHub and similar sites, though they ultimately ceased the attack without changing GitHub's behavior.[43]

Cyber capabilities, in some circumstances, can send a signal threatening greater non-cyber cost imposition. For example, a nation may reveal a cyber operation to another state as a means of showing that it can access the latter's strategically important networks. While it is unclear if Stuxnet was intended to have such a psychological effect, apparently the program introduced doubt into the minds of Iranian engineers, and the worm's revelation potentially impacted later nuclear negotiations.[44] In other cases, cyber capabilities—such as the capacity to send a message to anyone entering a certain area—can directly carry a warning. In 2014 protestors in Kiev received text messages of this sort.[45]

Nonlethal weapons and cyber capabilities are similar in that deployment of some forms of each can enable various kinds of deterrence. But a key difference emerges: nonlethal weapons, because they are more limited in their potential damage, are seldom the objects of deterrence. While hypothetically possible, it seems impractical for one entity to devote resources to deter another's employment of nonlethal weapons. The stakes are usually just too low. The threat of nonlethal weapons against American troops is not sufficiently serious to warrant either issuing powerful threats to impose costs or creating sufficient defenses to deny an adversary's benefit.

However, it is somewhat easier to conceive of situations where the United States might wish to deter another entity's use of nonlethal weapons by implementing denial. For example, if US forces embarked on a stabilization mission

© 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.

where the local population had demonstrated a desire or capability to employ nonlethal weapons, the United States might wish to demonstrate powerful defenses that easily blunt the effectiveness of those weapons.

Cyber capabilities, because they are potentially more destructive or—in the case of data theft—strategically damaging without being destructive, are different in kind. Nonlethal weapon deterrence yields a one-way question: How can nonlethal weapons be useful for deterrence? Cyber deterrence yields a two-way question: How can cyber capabilities be useful for establishing deterrence generally, and how can an adversary's use of cyber capabilities be deterred but not necessarily with cyber means?

As a result, the analogy between the two is attenuated. When asking how to deter the use of cyber capabilities by others, it is important not to limit oneself to thinking of one's own cyber capabilities. All elements of national power, including political clout, economic sanctions, kinetic retaliation, and cyber defenses, should be included in the deterrence discussion. Offensive cyber capabilities may be part of this calculus, but many are likely too subtle or too limited to fully act as a deterrent on their own. The analogy to nonlethal weapons here points to the need for a broader discussion of cyber deterrence.

Conclusion

A clear theme runs through this analysis: areas of overlap in both characteristics and in function exist between nonlethal weapons and cyber capabilities. These areas of overlap strengthen the case for the proposed analogy and point to the possibility that lessons learned about nonlethal weapons may be usefully applied to cyber capabilities. In short, recognizing how new and different cyber capabilities are, we need not consider them with an entirely blank slate. Analogizing to nonlethal weapons can be a valuable approach.

With that said, some cyber capabilities do not fit the analogy particularly closely—for example, those capabilities that do not seek to incapacitate a target (instead, they might steal data from it), those capabilities that do not seek to minimize collateral damage, and those capabilities that are irreversibly destructive. For discussions of these kinds of capabilities, nonlethal weapons are less obviously useful.

Another, more practical kind of limitation to this analogy concerns the employment of these weapons and capabilities. For reasons that remain largely elusive to the authors, the use of nonlethal weapons by US military forces has been restricted. Several military officers have informally observed and stressed that gaining authorization to employ lethal force was often easier than that for nonlethal force despite the latter's promise of lower collateral damage and only temporary effects. The question that remains unanswered in our research is, why are nonlethal weapons not better integrated and employed?

Further research into this question may be aided by bringing in literature on path dependency and the "stickiness" of entrenched traditions—or, in this case, the greater familiarity of employing kinetic, conventional weapons. Additional

© 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.

research may also tell us more about the inflexibility of military targeting procedures, which may have been designed to weigh specific variables in the context of a kinetic action but may be insufficiently malleable to more completely consider the authorization of nonlethal capabilities. These questions are important to examine, as they may tell us about the willingness and the process to employ cyber capabilities in the future.

Any answer to this question is going to depend on the type of nonlethal weapon in question and on the nature of the international legal regime that restricts those weapons. For example, the United States does not use riot-control agents in combat due to its commitments under the Chemical Weapons Convention.[46] Nor does the United States employ lasers to blind individuals, in compliance with the terms of the 1980 Convention on Certain Conventional Weapons.[47]

Further exploration of why nonlethal weapons have been deployed so seldom by US forces should be considered separately in more detail. For our purposes, it is worth noting that the lack of explicit international law around the employment of cyber capabilities may enable commanders to deploy possible future tactical capabilities with more freedom than they have with nonlethal weapons. In addition, cyber capabilities are—at least up until now—counter-matériel capabilities. Nonlethal weapons are both counter-matériel and counter-personnel. As such, the focus of cyber capabilities on counter-matériel missions may eventually give leaders less cause to eschew authorizing their tactical employment. This distinction may change, however, as wearable and related technologies create a new attack vector and open the possibility of cyber capabilities becoming counter-personnel capabilities.

Regardless of the reasons that inform the US military's decision to employ nonlethal weapons in only a limited fashion, practitioners would be wise not to take the nonlethal-cyber analogy too far for fear that, for whatever reason, cyber capabilities might become another instrument of power that is unwieldable even when they are the most appropriate tools available.

Indeed, despite very real concerns about a coming conflict in cyberspace, some of the most promising features of cyber capabilities are also common with other nonlethal weapons: their effects need not be permanent and could possibly be so narrowly tailored that collateral damage is all but eliminated. As with any other instrument of military power, cyber capabilities should be used only as a last resort. But when military coercion is required to secure US interests, cyber capabilities—like nonlethal weapons—may offer US military commanders the opportunity to do so in ways that greatly reduce the incidence of death and destruction on all sides of a future conflict.

Notes

The views expressed in this publication are those of the authors and do not necessarily reflect the official policy or position of the Department of Defense or the US government.

1. Joseph Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (Winter 2001); Joseph Nye, "Cyber Power" (Boston: Belfer Center for Science and

© 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.

International Affairs, May 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf; and Emily Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014).

2. Michael S. Goodman, "Applying the Historical Lessons of Surprise Attack to the Cyber Domain: The Example of the United Kingdom," in Goldman and Arquilla, *Cyber Analogies*; Nye, "Cyber Power"; Joel Brenner, *Glass Houses* (New York: Penguin, 2014); and Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010).

3. Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," The White House Blog, April 28, 2014, http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities; and Richard Clarke et al., "The NSA Report: Liberty and Security in a Changing World," President's Review Group on Intelligence and Communications Technologies (Princeton: Princeton University Press, 2013).

4. Rolf Weber, "Internet of Things: New Security and Privacy Challenges," *Computer Law & Security Review* 26, no. 1 (2010); and Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

5. The *Oxford English Dictionary* states that a weapon is "a thing designed or used for inflicting bodily harm or physical damage."

6. Ashton B. Carter, "DOD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy," Number 3000.03E (Washington, DC: Department of Defense, April 25, 2013), 12, http://www.dtic.mil/whs/directives/corres/pdf/300003p.pdf.

7. Leo P. Brophy, Wyndham D. Miles, and Rexmond C. Cochrane, *The Chemical Warfare Service: From Laboratory to Field*, United States Army in World War II (Washington, DC: Center of Military History, US Army, 1988).

8. Ibid., 2.

9. Ibid., 12.

10. Ibid., 70.

11. Ibid., 24.

12. Ibid., 25.

13. To characterize the overall effect of chemical weapons in World War I as nonlethal would be misleading, as the United Nations Office for Disarmament Affairs notes that chemical weapons employed in that conflict eventually killed more than 100,000 individuals. See United Nations Office for Disarmament Affairs, "Chemical Weapons," https://www.un.org/disarmament/wmd/chemical/.

14. United Nations Office for Disarmament Affairs, "Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare," 1925, https://www.un.org/disarmament/wmd/bio/1925-geneva-protocol/.

15. Brophy, Miles, and Cochrane, *Chemical Warfare Service*, 72–73.

16. Smoke is a nonlethal weapon, according to the definition used in this chapter, as it does not directly inflict bodily harm or physical damage. This reference is merely to note the evolution of how chemicals came to be used in World War II. Brophy, Miles, and Cochrane, *Chemical Warfare Service*, 197.

17. Ibid., 197–225.

18. Gerald Ford, "Executive Order 11850—Renunciation of Certain Uses in War of Chemical Herbicides and Riot Control Agents," *Federal Register*, April 8, 1975, http://www.archives.gov/federal-register/codification/executive-order/11850.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.

19. Andrew Sanders and Ian S. Wood, *Time of Troubles: Britain's War in Northern Ireland* (Edinburgh: Edinburgh University Press, 2012), 127.

20. Richard Pike, *Phantom Boys: True Tales from Aircrew of the McDonnell Douglas F-4 Fighter-Bomber* (London: Grub Street Books, 2015), 105.

21. Barton Reppert, "Force without Fatalities," *Government Executive*, May 1, 2001, http://www.govexec.com/magazine/magazine-defense/2001/05/force-without-fatalities/8992/.

22. Senate Armed Services Committee, *Nomination of Maj. Gen. Anthony C. Zinni, USMC, for Appointment to the Grade of Lieutenant General and to Be the Commanding General, 1st Marine Expeditionary Force*, 103rd Cong., 2nd sess., June 16, 1994, Hrg. 103–873, 32.

23. Richard L. Scott, "Conflict without Casualties: Non-Lethal Weapons in Irregular Warfare" (thesis, Naval Postgraduate School, 2007), 6–7.

24. Nick Lewer and Steven Schofield, *Non-Lethal Weapons: A Fatal Attraction?* (London: Zed Books, 1997), 20.

25. For more on this episode, see F. M. Lorenz, "Non-Lethal Force: The Slippery Slope to War?," *Parameters*, 1996, 52–62.

26. Reppert, "Force without Fatalities."

27. Graham T. Allison and Paul X. Kelley, "Nonlethal Weapons and Capabilities" (Washington, DC: Council on Foreign Relations, 2004), 13–18.

28. Ibid., 1.

29. For one of the earliest articulations of this idea, see David D. Clark and David R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy*, 1987, 184–94.

30. John Leyden, "Israel Suspected of 'Hacking' Syrian Air Defences," *The Register*, October 4, 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

31. Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg, December 11, 2014, http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

32. Dan Kloeffler and Alexis Shaw, "Dick Cheney Feared Assassination via Medical Device Hacking: 'I Was Aware of the Danger,'" ABC News, October 19, 2013, http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434.

33. Weber, "Internet of Things"; and Greenberg, "Hackers Remotely Kill."

34. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 97.

35. Ibid.

36. Ibid.; and Kasperky Lab, "Gauss: Abnormal Distribution," SecureList, August 9, 2012, https://securelist.com/analysis/publications/36620/gauss-abnormal-distribution/.

37. Rachel King, "Stuxnet Infected Chevron's IT Network," *Wall Street Journal*, November 8, 2012, http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.

38. Zetter, *Countdown to Zero Day*.

39. For a sampling of perspectives, see Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?," *Strategic Studies Quarterly*, Fall 2010, 102–35; Murat Dogrul, Adil Aslan, and Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *2011 3rd International Conference on Cyber Conflict*, ed. C. Czosseck, E. Tyugu, and T. Wingfield (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2011), 43; and Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (2010).

© 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.

40. To be sure, the United States also sought to deter the Chinese from undertaking similar activity, but in large part the goal was to influence the perceptions of the Soviet leadership that it should not undertake a nuclear-armed attack.

41. For a fuller explication of the two variables here—absolute versus general deterrence and specific versus restrictive deterrence—and an application to cyber operations, see Ben Buchanan, "Cyber Deterrence Isn't MAD; It's Mosaic," *Georgetown Journal of International Affairs*, International Engagement on Cyber IV, 15, no. 2 (2014): 130–40.

42. See also how the concept of entanglement relates to the calculation of an action's costs. Joseph Nye, "Can China Be Deterred in Cyber Space?," Foreign Policy Association (blog), April 6, 2016, http://foreignpolicyblogs.com/2016/04/06/can-china-be-deterred-in-cyber-space/.

43. Bill Marczak et al., "China's Great Cannon," Research Brief (Citizen Lab and Munk School of Global Affairs, University of Toronto, April 10, 2015), https://citizenlab.org/2015/04/chinas-great-cannon/.

44. David Sanger and William Broad, "Unstated Factor in Iran Talks: Threat of Nuclear Tampering," *New York Times*, March 21, 2015, http://www.nytimes.com/2015/03/22/world/middleeast/unstated-factor-in-iran-talks-threat-of-nuclear-tampering.html.

45. Heather Murphy, "Ominous Text Message Sent to Protesters in Kiev Sends Chills around the Internet," *New York Times*, January 22, 2014, http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/.

46. Allison and Kelley, "Nonlethal Weapons and Capabilities."

47. Ibid., 53.

© 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.

UNDERSTANDING CYBER CONFLICT

14 ANALOGIES

GEORGE PERKOVICH
ARIEL E. LEVITE
EDITORS

Georgetown University Press / Washington, DC

© 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.

© 2017 Georgetown University Press. All rights reserved. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage and retrieval system, without permission in writing from the publisher.

The publisher is not responsible for third-party websites or their content. URL links were active at time of publication.

Library of Congress Cataloging-in-Publication Data

Names: Perkovich, George, 1958- editor. | Levite, Ariel, editor.
Title: Understanding cyber conflict : fourteen analogies / George Perkovich and Ariel E. Levite, editors.
Description: Washington, DC : Georgetown University Press, 2017. | Includes bibliographical references and index.
Identifiers: LCCN 2017003096 (print) | LCCN 2017008146 (ebook) | ISBN 9781626164987 (pb : alk. paper) | ISBN 9781626164970 (hc : alk. paper) | ISBN 9781626164994 (eb)
Subjects: LCSH: Cyberspace operations (Military science)
Classification: LCC U167.5.C92 U54 2017 (print) | LCC U167.5.C92 (ebook) | DDC 355.4--dc23
LC record available at https://lccn.loc.gov/2017003096

♾ This book is printed on acid-free paper meeting the requirements of the American National Standard for Permanence in Paper for Printed Library Materials.

18 17 9 8 7 6 5 4 3 2 First printing

Printed in the United States of America

Cover design by Jen Huppert. Cover image by robertiez/iStockphoto.

© 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.