Aviation electronics technician 3rd class conducts maintenance on aircraft targeting systems in aircraft intermediate maintenance department maintenance shop on USS *Ronald Reagan*, Philippine Sea, July 25, 2020 (U.S. Navy/Jason Tarleton)

Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat

By Josiah Dykstra, Chris Inglis, and Thomas S. Walcott

Dr. Josiah Dykstra is a Technical Fellow in the Cybersecurity Collaboration Center at the National Security Agency. Chris Inglis is the Robert and Mary M. Looker Professor in Cyber Security Studies at the U.S. Naval Academy. Thomas S. Walcott is the Technical Director in the Cyber National Mission Force at U.S. Cyber Command.

Warfare, with a history as old as humanity itself, has been predominantly conducted through the application of physical force to disrupt, degrade, or destroy physical assets. That long history has led to well-developed doctrine and principles for shows of force, deterrence, proportionality, and rules for warfare that rely on predictable and repeatable characteristics of the physical weapons employed. The advent of cyber warfare in the modern era, however, has illustrated that the assumptions used for the employment of kinetic weapons do not necessarily apply to the employment of cyber capabilities. For example, unlike a physical missile or bomb, it is difficult to predict the precise effects, measure the resulting proportionality, or estimate the collateral effects attendant to the use of a computer virus. As we discuss, the differences between kinetic weapons and cyber weapons are discernible, manageable, and have far-reaching implications for strategic military doctrine, planning, and operational employment in both power projection and defense.

In order to wage and win modern conflict, the attributes of kinetic and

cyber weapons must be fully understood singly and in combination. To date, discussion and debate about the attributes of cyber weapons have focused on a few basic characteristics, such as *perishability*—that is, making it difficult to achieve the same precision, let alone confidence, that typically results from the use of kinetic weapons. For military leaders, and the policymakers who determine the purposes and applications of military power, the differences between kinetic and cyber weapons prompt a reevaluation of how these individuals employ weapons and measure their effectiveness, which foundationally relies on a clear articulation of differences and similarities between the kinetic and cyber environments. We propose and describe a strategic framework, though not exhaustive, that could be applied to any instrument of power employed by a nation-state; we then describe distinctions between kinetic and cyber weapons to draw out both differences and strategic implications.

This article compares instruments of offensive kinetic and cyber power across three key areas: weapons characteristics, targeting, and policy/practice.[1] These thematic categories emerged as we identified 18 individual differences between kinetic and cyber weapons. The weapons characteristics category includes differences in the inherent properties of the weapons as well as in the effects they can deliver. The targeting category highlights divergences in how the weapon influences target selection and pursuit. The policy and practice category covers differences in the current environment and maturity of the weapons.

As we unpack these areas, military leaders should keep in mind three framing questions that can help guide the selection and application of any weapon and that apply equally well to kinetic and cyber:

- Is the weapon able to achieve the desired effect within the constraints of time available for planning and execution, the professional skills of the human operators, and materiel resources?
- Is it possible to limit the weapon's effects to those desired with acceptable impact to innocent parties and assets?
- Will the use of the weapon contribute to, or risk undermining, stability, the ability of the employing organization to manage escalation, and/or other desired characteristics of adversary engagement?

The answers to these questions depend, in part, not only on situational factors but also on a firm understanding of weapon nuances. We draw out those details in the following sections.

To frame the discussion, we must consider the weapons' definitions. Unfortunately, the Department of Defense (DOD) does not explicitly define *weapon* in doctrine, though DOD does use the word within other definitions. We start, therefore, with a dictionary definition for *weapon* as "an instrument of any kind used in warfare or in combat to attack and overcome an enemy."[2] Notably, weapons are traditionally employed to create both lethal and nonlethal effects. Joint Publication (JP) 3-12, *Cyberspace Operations*, defines *cyberspace capability* as "a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace."[3] For the purposes of this discussion, we consider a cyberspace capability distinct from (yet predicated on) some mechanism that enables access to the system within which the intended effect will be achieved. JP 3-0, *Joint Operations*, acknowledges that cyberspace attack is one capability that could create nonlethal effects; other examples include electronic attack, military information support operations, and nonlethal weapons. The military action known as *fires*, states JP 3-0, is to "use available weapons and other systems to create a specific effect on a target."[4] Cyberspace attack actions are a form of fires and "create noticeable denial effects (that is, degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains."

In the following sections we introduce and differentiate 18 characteristics that are grouped as differences in weapons characteristics, targeting, and policy and practice between cyber weapons and their kinetic counterparts. The table summarizes these differences.

Differences in Weapons Characteristics

Many discussions about cyber weapons have focused on the basic attributes of the cyber domain, such as the global interconnected network; the highly fluid interplay of its constituent components of hardware, software, and configuration; and the resulting fragility of access paths needed by cyber operators to reach their intended targets. Contemporary discussions of cyber weapons have also explored their high degree of perishability and rapid obsolescence.[5] These traits are becoming commonly understood today but are alone insufficient to allow for a comparison of cyber and kinetic weapons. The additional differences below can aid tactical and strategic thinking.

Kinetic weapons typically generate access and effect (by *force*) nearly instantaneously, while cyber weapons necessarily separate access and effect into two distinct actions, often divided by a significant expanse of time (in some cases, cyber access is developed weeks or months in advance of the intended effect). In the Joint Operational Access Concept, the phrase *operational access* is defined as "the ability to project military force into an operational area with sufficient freedom of action to accomplish the mission."[6] Kinetic weapons can produce such access for force projection and provide antiaccess and area denial against opposing forces. Cyber weapons typically separate access from effect, and they often require a significant effort to construct access tailored to the given target and its environment. For example, denial-of-service attacks leverage the access provided by a path from the aggressor to functioning networks. Data destruction attacks control access provided by another means, such as remote exploitation or social engineering, but the key to their success remains an access path from the attacker to the intended target. The

Gunner and cannon crewmember, assigned to Chaos Battery, 4th Battalion, 319th Airborne Field Artillery Regiment, 173rd Airborne Brigade, dials in target of M777 Howitzer during live-fire exercise as part of Saber Junction 19, at 7th Army Training Command's Grafenwoehr Training Area, Germany, September 11, 2019 (U.S. Army/Thomas Mort)

implication is that cyber weapons require significant tailoring, prepositioning, and/or bundling with a target-specific, access-creating capability.

Kinetic weapons almost always produce irreversible physical effects, whereas cyber weapons can produce completely reversible effects. Although a small fraction of weapons (for example, rubber bullets) can deliver a quickly recoverable outcome, most are intended to produce permanent or slow-recovery effects. While cyber weapons can produce permanent damage to the physical world—such as in the case of Stuxnet, which caused physical destruction of centrifuges—other cyber effects can be completely reversed by either the attacker or the victim. For example, when a denial-of-service attack stops, the target systems return to normal. Encryption, such as used in ransomware, is also reversible given the correct decryption key. Indeed, ransomware relies on reversibility in order to be effective; demonstration of the capability to deny access and the subject's belief that it can be undone are the predicate to the victim's willingness to pay ransom. Importantly, reversibility can be an asset or limitation of cyber weapons, depending on the objective of their use.[7]

It is difficult to reverse-engineer and reuse kinetic weapons, since they are typically damaged beyond reuse as a condition of their employment. Because cyber weapons are often comprised of easily replicable software, they offer more ability for others to observe, analyze, and reuse the weapon by simply copying the software and replaying the context of its employment. Given the previously described time delay in constructing access and effecting employment of the cyber weapon, many cyber attacks can be observed and copied using playback capabilities of digital systems designed to monitor the flow and storage of data and software, even if it requires the cyber attack to highlight the significance of a recorded session. The result is a high likelihood that the cyber weapon will be copied intact and studied by an adversary, even if the capture itself is after the attack. Some experts have compared this situation to living in a glass house, arguing that the use of cyber for offense necessitates the preparation and deployment of defenses from the adversary repurposing the weapon against the attacker.[8] In the physical world, weapons platforms can be kept at a distance from their target and thereby protected from harm. Ammunition from kinetic weapons is expendable and, once expended, is generally difficult, impossible, or pointless to reconstruct and replay.[9]

Although in the physical world some weapons—including nuclear, biological, and chemical—challenge weaponeers' abilities to precisely constrain the physical impacts when employed, kinetic weapons typically have a quantifiable local effect governed by attributes of the physical world. And while a nuclear device cannot be configured to destroy only the brick buildings in a particular area, it could be configured and employed to constrain its effects to a physical region. Cyber effects, however, may deliver both local and cascading effects, determined through configuration of the weapon, the target, and the domain of cyberspace. Across the relatively brief span of the history of cyber weapons' employment, seemingly localized domain and network hijacking attacks have often affected the global Internet. The Petya attack attributed to Russia in summer 2017 is an excellent case in point. Though generally assessed to be an attack by Russia on government systems operated by Ukraine,[10] the strike quickly spread to nongovernmental systems across Europe—in one case knocking out most of the global information technology system and associated global command and control of the Maersk shipping line, among many other widespread effects felt well outside Ukraine.[11]

Table. Differences Between Kinetic and Cyber Weapons

	Kinetic Weapons	Cyber Weapons
Weapon	Generate access	Leverage access
	Difficult to reverse-engineer and repurpose	Use may result in others adopting it too
	Permanent effect	Potentially reversible effects
	Local effect	Possible global effect
	Consistent effect	Variable effect
	Scale with volume	Scale with use
	Fixed effect	Tailorable effect
	Predictable effect and effectiveness	Sensitive to environmental changes
	High barriers for entry	Low barriers for entry
Targeting	One weapon, one target	One weapon, many targets
	Minimal geographic prepositioning	Can be significant prepositioning (system-specific)
	Positive control	Opportunistic
	Coarse targeting	Surgical targeting
Policy and Practice	Significant experience	Little experience
	Unambiguous intent	Potentially ambiguous intent
	Limited value below level of armed conflict	Useful in all levels
	Overtly attributable	Tailorable attribution
	Confident	Mixed confidence

Kinetic weapons deliver consistent, fixed effects that correspond with the attributes of the weapon in a world where the physical properties of the target and its environs, such as gravity and air density, are relatively stable. The same cyber weapon could potentially be used for variable effect, depending on the nuances of coding from subtle (so-called spyware) to dramatic (ransomware). Similarly, a fixed kinetic effect means that outcomes cannot be tailored to a target. Cyber weapons are malleable and can be easily changed or tailored with high granularity to produce a custom effect on only a specific device or chip.

Modern military operations require agility and adaptability in plans and crisis response, including the flexibility to scale operations up and down. Scaling the effects from kinetic attacks generally comes from increasing the literal number, or volume of the payload, of weapons deployed. Because ammunition is expendable, one kinetic weapon at the point of delivery impacts one target. And while the number of kinetic payloads delivered in an area can be increased, there is generally a correlation between payload mass, velocity, and kinetic effect. A single cyber weapon could be used against one or many targets simply by coding the weapons effects, thus enabling inherent and impressively responsive scalability. Ransomware is one example of the same cyber weapon reused against many targets. A defensive corollary is that defending against kinetic weapons requires a per-instance cost. Scaling defense for many targets against a cyber weapon, such as with antivirus software, is comparatively more cost effective.[12]

Military planners likewise benefit when given choices across a spectrum of effects. Kinetic weapons offer fixed effects; that is, the effect is predetermined at the time a given weapon is created. Cyber weapons could also be created with a prescribed action or outcome but are likely to offer a tailorable effect at the time of employment. One can easily imagine that a weapon capable of deleting a specific file could be rapidly and easily tailored to delete any or many other files. A consequence is that more preparation may be necessary to offer equivalent preparedness and confidence in defending against the cyber weapon.

Kinetic weapons can yield predictable outcomes because the relevant variables influencing the outcomes are well understood. The laws of physics and their effect on kinetic weapons have been studied and documented, and environmental changes have highly predictable and quantifiable impacts on the effectiveness of a kinetic weapon. Cyber effects are extremely sensitive to changes in the environment, from subtle changes in the target's software, hardware, or user settings, to dynamic global networking that serves as the connection between attacker and target. Small, potentially unobserved changes to software or networking could significantly impact the effectiveness of a cyber weapon that relies on very specific software settings.

Finally, we note the difference in the accessibility of kinetic and cyber weapons. Today, entry-level cyber weapons are

Marines with Marine Corps Forces Cyberspace Command in operations center at Lasswell Hall aboard Fort Meade, Maryland, February 5, 2020 (U.S. Marine Corps/Jacob Osborne)

increasingly common as a commodity widely shared by aggressors of varying technical capability. The pervasive availability, low cost, and low expertise necessary to operate them mean that cyber weapons could be employed by many state and nonstate actors. Tools that are freely available (for example, the widely available Metasploit) or on the open market (Core Impact) are easily weaponized for cyber attack. For the United States, this situation is both a liability, in effectively arming more adversaries through the increased exposure of U.S. cyber weapons, and a potential opportunity, by raising the cost to adversaries of conducting cyber attacks by forcing them to counter the greater number of platforms that economies of scale allow the United States to bring to bear. In general, large-scale kinetic weapons, conversely, continue to remain out of reach in cost, expertise, or availability to many adversaries.

Differences in Targeting

The first difference in the targeting category is in the weapon-to-target ratio. At the point of impact, a kinetic weapon is intended for a single target. Although the scope and scale of the target may vary, even kinetic weapons of mass destruction are limited in time and space. Conversely, cyber weapons offer an ability to affect many targets across time and space, in some cases leveraging each target as the launch platform for the next. Cyber weapons are not expended on use unless someone develops an inoculation, such as a patch—and even in that case, the inoculation may not be global.

Another important distinction is the standoff range from the target. Kinetic weapons can be effective with minimal prepositioning relative to the target—this is particularly true for kinetic weapons of long geographic range. Physical geography matters much less in cyberspace, but the complex digital environment often demands significant prepositioning and initial preparation of the battlespace before the cyber weapon can reach the target.

Targeting is affected by the degree of control over the target (the *find and fix* problem) and the weapon (the *finish* problem). Precise targeting and positive control over the selection of targets for delivery of effects are important to achieving military objectives and avoiding collateral damage. Cyber weapons may require a mix of opportunistic and

discriminating targeting. Stuxnet is a case study where the weapon was designed to roam across many systems, infecting those that met the target criteria while bypassing those that did not.[13] This is an example of opportunistic access as opposed to positive control over the systems infected. It further illustrates the difference between access and effect.

Drawing distinctions in the granularity and precision allowed by kinetic or cyber weapons makes it easy to highlight the difference between the coarse targeting and surgical effect of cyber weapons. Stuxnet had a surgical effect against specific targets, coupled with (comparatively) coarse targeting for access. Precise targeting requires good technical design and good intelligence.[14] There are few, if any, kinetic weapons that can operate with coarse access and surgical effect.

Differences in Policy and Practice

Today, the accumulated experience with cyber weapons has not yet achieved the same maturity as that with kinetic weapons. There is a robust wealth of experience in the development, analysis, and use of kinetic weapons; most have evolved slowly over decades or centuries of refinement and application. The Joint Technical Coordinating Group for Munitions Effectiveness, for example, was established in 1964 to provide weapons effectiveness data in joint munitions effectiveness manuals. No such structure exists for cyber weapons. Furthermore, militaries have extensive experience, including training, in employing kinetic weapons. The relatively recent emergence of cyber weapons has not yet had sufficient time to produce the same amount of experience. As a result, hesitance and uncertainty about integrating cyber as a strategic weapon remain.

When weapons are deployed, their use conveys a message to the adversary. The intent behind the use of kinetic weapons is nearly always unambiguous. The escalation of conflict means that both sides understand, on some level, what the other seeks to achieve through the conflict. The use of force is the last resort for modern nations. Cyber weapons, however, can convey ambiguous messaging, either in their intended effect or in their linkage to a particular actor (the attacker) or a discernible campaign. This situation might be preferred if the cyber weapon was an enabler for an integrated kinetic attack; it could be most undesirable if the cyber attack was the main effort in a campaign designed to impose costs and message the adversary.

Cyber weapons offer unique value in all stages of conflict and confrontation, and they can be particularly effective when employed below the level of armed conflict. Continuous global gray zone conflict in cyber exchanges is likely to occur for the foreseeable future.[15] Kinetic weapons, conversely, are by definition not employed outside of armed conflict—this may be the most distinguishing and important difference between kinetic and cyber weapons. In June 2019, the press reported that U.S. Cyber Command (USCYBERCOM) carried out cyber attacks against Iran in response to Iranian aggression.[16] Although the attack was coordinated with plans for kinetic weapons, the cyber option was executed because the United States apparently elected not to exercise kinetic options. This scenario may demonstrate that cyber was a less escalatory, nonkinetic option that still provided a response and message to Iran.

For nation-states, kinetic weapons carry an overt attribution of the instigator. Attribution in cyberspace remains a difficult problem, as tools and infrastructure are easily obfuscated and manipulated.[17] Cyber weapons, therefore, offer customized attribution. Revealing attribution at a time of the attacker's choosing is a powerful capability.

Humans, including leaders and decisionmakers, weigh their choices, in part, according to their confidence in the options available. Modern military leaders have high confidence in kinetic weapons, owing to experience and training. Today, cyber weapons bring mixed confidence in the effects and effectiveness of the weapons. Persistent operational engagement, combined with science and technology in modeling and simulation, will help build the experience necessary to grow confidence in their effectiveness.

Evolution of Cyber Weapons as a Strategic Capability

Comprehensive national security requires the consideration and coordinated use of all instruments of power across every phase of conflict. It is important to highlight that cyber has only recently emerged as a full instrument of power and strategic capability for the United States. This development was possible given a confluence of deliberate thought and exploration, as well as significant milestones in law, policy, and strategy, but much work remains to elevate cyber's maturity to the level long enjoyed by the kinetic realm of warfare. The growing maturity, especially in the area of policy and practice, will continue to shape the future of integrated warfare.

In 2018, the Defense Science Board (DSB) Task Force on Cyber as a Strategic Capability determined that DOD "must move beyond tactical applications for cyber and realize cyber as a strategic capability."[18] The task force was also asked to compare cyber with kinetic capabilities, including unintended consequences and collateral damage. Key conclusions of the DSB's final report were that, regardless of the means employed to generate a given effect, a strategic capability had the following generic attributes:

- The capability can create a discernible, and preferably enduring, effect on a target's materiel, efficiency, and/or will (that is, the adversary respects and is influenced by the capability).
- The capability is sufficiently well developed and mature that it can generate the desired effect within a reasonable time of a stated need (that is, it is responsive to policy and combatant commander needs).
- The capability can be regenerated within a reasonable time (that is, it can support campaigns in addition to one-time [tactical] strikes).

Four milestones over the past 2 years were instrumental in transforming this

Air Force special tactics operators cross field to approach second target building during operability training at Eglin Range, Florida, April 22, 2020 (U.S. Air Force/Rose Gudex)

aspiration to reality. National Security Presidential Memorandum 13, *U.S. Cyber Operations Policy*, provided the necessary policy,[19] the National Defense Authorization Act for fiscal year 2019 provided the statutory basis,[20] and the DOD Cyber Strategy provided the doctrine.[21] Furthermore, USCYBERCOM was elevated to a combatant command, and its present commander, General Paul Nakasone, USA, has begun to employ these newly assigned authorities under the doctrine of persistent engagement.[22] These milestones demonstrate that the United States is willing and able to employ cyber capabilities, albeit in combination with other capabilities, to protect itself in and through cyberspace.

The Future of Integrated Kinetic and Cyber Combat

The ability to win and prevent modern wars brings an urgent need to understand the unique risks and opportunities of integrated kinetic and cyber warfare. Cyber attacks, independent from kinetic action, are increasingly common, supported by nation-states, and undertaken by independent actors. Yet even conventional warfare is beginning to integrate cyber capability—for example, Russia's invasion of Ukraine was preceded by cyber attacks against critical infrastructure. The United States must quickly learn to integrate cyber capabilities to the greatest possible effect.

The differences between kinetic and cyber weapons explored in this article demonstrate that the capabilities are distinct but complementary and potentially multiplicative in impact when applied in combination. Some researchers have hypothesized that integrating the weapons will even present new and expanded options for military power. JP 3-12 appears to support this assertion, stating that "cyberspace attack capabilities, although they can be used in a stand-alone context, are generally most effective when integrated with other fires."[23] At present, there is insufficient experience to validate that claim other than intuition. Cyber and kinetic weapons can be incredibly powerful on their own and can achieve a desired military outcome independently. If the ideal of military dominance is to avoid armed conflict altogether, cyber capabilities present unique opportunities to produce a wide range of effects.

Nuanced insight about the differences between weapons allows military leaders to more fully integrate kinetic and cyber. Apart, the kinetic and cyber domains may not deter or stop a modern adversary. New options must be made with respect to the differences between the domains. The military is beginning to learn how, where, and when to use cyber weapons. That knowledge will then allow leaders to determine if these domains could be leveraged in a complementary fashion.

Many open questions remain about the integration of kinetic and cyber combat. By presenting an even broader scope of possible effects, hybrid kinetic-cyber weapons systems and operations raise new questions about the practice of warfare. Unmanned systems are an illustrative example of an integrated weapon: cyber control systems with kinetic effects. The kinetic munition on a drone displays the corresponding kinetic characteristics, including a fixed, predictable, and permanent effect. Targeting, policy, and practice likewise seem to correspond with the offensive attributes of kinetic weapons; however, an adversary targeting the drone or its control system could theoretically produce a tailored, variable, reversible, misattributable effect. Unlike a physical attack against the drone, these attributes complicate the ability to prove that an adversary seized control of the unmanned system; this could delay a defensive response. Unmanned systems also raise questions about what constitutes a valid military target: Is it the remote operator? The location of the operator? The carriers of communications between the operator and the drone? The developers of components of the weapons system?

Whether separately or combined, cyber and kinetic weapons are now available as strategic instruments of power and present novel opportunities for pursuing national objectives. Given the short history of cyber warfare, many opportunities remain for future work to deepen the understanding of cyber weapons. As leaders gain experience and expertise with cyber weapons, integrated combat and gray zone options will be strengthened. The differences in kinetic and cyber weapons outlined in this article are a necessary foundation to understand and leverage the unique and integrated qualities of cyber capabilities. **JFQ**

Notes

[1] While we principally focus on offensive (deny, degrade, disrupt, destroy, and manipulate) capabilities throughout this article, cyber and kinetic effects are also successful for defense and deterrence; these are widely discussed in the literature. Cyber deterrence has been the focus of significant academic and governmental research, making it an area where both practice and theory are rapidly evolving. See, for example, Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), 381–393, available at <www.sciencedirect.com/science/article/pii/S0030438717300431>. See also Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Department of Defense, February 2017), available at <https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf>.

[2] "Weapon," *OED Online*, Oxford University Press, June 2019.

[3] Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), I-4, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf>.

[4] JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, October 22, 2018), III-30, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf>.

[5] Christopher A. Bartos, "Cyber Weapons Are Not Created Equal," U.S. Naval Institute *Proceedings* 142/6/1 (2016), 30–33, available at <https://calhoun.nps.edu/handle/10945/49618>.

[6] *Joint Operational Access Concept*, Version 1.0 (Washington, DC: The Joint Staff, January 17, 2012), ii, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joac_2012.pdf>.

[7] See also N.C. Rowe, "Towards Reversible Cyberattacks," in *Proceedings of the 9th European Conference on Information Warfare Security*, ed. Josef Demergis (Thessaloniki, Greece: University of Macedonia, 2010).

[8] Eric Rosenbach, *Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks*, Testimony Before the Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, June 12, 2017, available at <https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf>.

[9] It is possible to imagine re-creating a bullet but hard to imagine the benefit of doing so. It is hard to imagine fully re-creating a missile after it has exploded.

[10] "Alert (TA17-181A): Petya Ransomware," U.S. Department of Homeland Security—Cybersecurity and Infrastructure Security Agency, July 1, 2017, available at <https://www.us-cert.gov/ncas/alerts/TA17-181A>.

[11] "Global Ransomware Attack Causes Turmoil," BBC News, June 28, 2017, available at <https://www.bbc.com/news/technology-40416611>.

[12] Two important notes: First, this presumes known weaponry (that is, the parameters are understood and defenses are known). Second, cyber weapons represent the code that produces the effect and are distinct from the access vector that enables the effect; defenses against the full spectrum of possible access vectors can be quite costly and might not scale well.

[13] Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (Arlington, VA: The Langner Group, November 2013), available at <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.

[14] Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3, no. 1 (March 2017), 59–68, available at <https://academic.oup.com/cybersecurity/article/3/1/59/3097802>.

[15] Defense Science Board, *Summer Study on Capabilities for Constrained Military Operations* (Washington, DC: Department of Defense, December 2016), available at <https://dsb.cto.mil/reports/2010s/DSBSS16_CMO.pdf>.

[16] Julian E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," *New York Times*, June 22, 2019, available at <www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html>.

[17] See Alexander Kott, Norbou Buchler, and Kristin E. Schaefer, "Kinetic and Cyber," in *Cyber Defense and Situational Awareness*, ed. A. Kott, C. Wang, and R.F. Erbacher (New York: Springer International Publishing, 2014), 29–45, available at <https://arxiv.org/pdf/1511.03531.pdf>.

[18] *Task Force on Cyber as a Strategic Capability: Executive Summary* (Washington, DC: Department of Defense, June 2018), available at <https://www.hsdl.org/?abstract&did=813604>.

[19] Joint Hearing to Receive Testimony on the Cyber Operational Readiness of the Department of Defense, Committee on Armed Services, Subcommittee on Cybersecurity, September 26, 2018, available at <https://www.armed-services.senate.gov/imo/media/doc/18-60_09-26-18.pdf>.

[20] H.R. 5515, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," available at <https://www.congress.gov/bill/115th-congress/house-bill/5515/text>.

[21] *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), available at <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>.

[22] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019).

[23] JP 3-12, V-19.