STRATEGIC STUDIES QUARTERLY

The Strategic Promise of Offensive Cyber Operations

Max Smeets

Abstract

Could offensive cyber operations provide strategic value? If so, how and under what conditions? While a growing number of states are said to be interested in developing offensive cyber capabilities, there is a sense that state leaders and policy makers still do not have a strong conception of its strategic advantages and limitations. This article finds that offensive cyber operations could provide significant strategic value to state-actors. The availability of offensive cyber capabilities expands the options available to state leaders across a wide range of situations. Distinguishing between counterforce cyber capabilities and countervalue cyber capabilities, the article shows that offensive cyber capabilities can both be an important force-multiplier for conventional capabilities as well as an independent asset. They can be used effectively with few casualties and achieve a form of psychological ascendancy. Yet, the promise of offensive cyber capabilities' strategic value comes with a set of conditions. These conditions are by no means always easy to fulfill—and at times lead to difficult strategic trade-offs.

❋ ❋ ❋ ❋ ❋

At a recent cybersecurity event at Georgetown Law School, Richard Ledgett, former deputy director of the National Security Agency (NSA), told an audience "well over 100" countries around the world are now capable of launching cyber-attacks.[1] Other senior policy makers and experts have made similar statements about the proliferation of offensive cyber capabilities.[2] Yet, offensive cyber operations are not considered to be an "absolute weapon," nor is their value "obviously beneficial."[3] There is also a sense that state leaders and policy makers, despite calling for

Max Smeets is a postdoctoral cybersecurity fellow at Stanford University Center for International Security and Cooperation (CISAC). He is also a nonresident cybersecurity policy fellow at New America and research associate at the Centre for Technology & Global Affairs, University of Oxford.

the need to acquire offensive cyber capabilities, do not have a clear conception of their strategic advantages.[4] Henry Kissinger in *World Order* writes that "internet technology has outstripped strategy or doctrine—at least for the time being. In the new era, capabilities exist for which there is as yet no common interpretation—or even understanding. Few if any limits exist among those wielding them to define either explicit or tacit restraints."[5] Former CIA and NSA director Michael Hayden notes in his book that "[f]rom their inception, cyber weapons have been viewed as 'special weapons,' not unlike nuclear devices of an earlier time. But these weapons are not well understood by the kind of people who get to sit in on meetings in the West Wing, and as of yet there has not been a Herman Kahn [of *On Thermonuclear War* fame] to explain it to them."[6] Similarly, former commander of the US Strategic Command James Ellis notes that the current strategic thinking on cyber conflict is "like the Rio Grande [River], a mile wide and an inch deep."[7]

This article offers more strategic scrutiny of offensive cyber operations. It does not aim to provide a descriptive or explanatory exercise, trying to understand why military cyber operations have been conducted in the past. Instead, it proposes the conditions under which these activities could effectively be conducted. After all, offensive cyber operations can only be successfully conducted in practice, once we have carefully considered the theoretical parameters of effectiveness.

The focus of this article is on a state actor in the international system that has established a well-resourced military cyber command (or equivalent) able to conduct a range of offensive cyber operations. Assuming a state is well resourced, this assessment underemphasizes the obstacles actors have to overcome to develop or acquire these capabilities.[8] It also excludes defender characteristics from this analysis and only assesses the value of these capabilities from the perspective of the state actor using these capabilities.[9] In addition, even though there is said to be an ongoing proliferation of capabilities to nonstate actors—worthy of analysis on their own terms—the state remains the principal legitimate actor to use these capabilities. Finally, an offensive cyber capability could potentially have strategic value short of actual use. Indeed, the coercion literature makes clear that a credible threat of military action could affect the behavior of other actors.[10] Even though these mechanisms could potentially be important, they are not part of the argument.

Unlike what some scholars and policy makers have suggested, offensive cyber operations could provide significant strategic value to state actors. The availability of offensive cyber capabilities expands the options available to state leaders across a wide range of situations. Offensive cyber capabilities can be both an important force-multiplier for conventional capabilities as well as an independent asset. They can be used effectively with few casualties and achieve a form of psychological ascendancy. However, the strategic value of different offensive cyber capabilities comes with a set of conditions. These conditions are by no means always easy to fulfill—and at times lead to difficult strategic trade-offs.

The article first addresses the strategic value offensive cyber operations. Then it clarifies the nature of offensive cyber operations, distinguishing between counterforce cyber capabilities (CFCC) and countervalue cyber capabilities (CVCC). Finally, it creates four propositions on the use of offensive cyber capabilities and specifies the conditions in which they could provide strategic value.

The Strategic Value of Offensive Cyber Operations

There is no single method to measure the strategic value of offensive cyber operations. Strategic value can mean at least two different things. First, it can refer to whether an offensive cyber operation can provide value in support of a national strategy.[11] The assessment of value then is highly dependent on defining what the strategy is. Following this perspective, one could, for example, analyze how offensive cyber operations contribute to the pursuit of deterrence—the most frequently referred-to strategy. Yet, it remains unclear to what degree deterrence (or any other strategy for that matter) is in fact the correct strategy to pursue.[12] Hence, if we use cyber deterrence as a measure, one may come to the conclusion that offensive cyber operations do have strategic value or they do not.[13]

Second, the term "strategic value" could also refer to cyber's ability to produce an outcome of conflict itself or, even more broadly, to state competition. Here, we use a different set of measures for "value": how the conduct of offensive cyber operations helps to avoid and/or affect the strategic outcome of a conflict.[14]

According to international relations scholar Erik Gartzke, "'cyber war' is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence."[15] Although offensive cyber capabilities should

not be conceived as the most authoritative asset, an analysis of their strategic value is nevertheless valuable. If one uses "final arbitration" as a criterion for analysis, almost no capability would pass the test. Hence, the approach here is more closely aligned with Colin Gray's review of military assets' strategic utility.[16] In the final part of his book *Explorations of Strategy* Gray writes the following about special operations: "[I] will avoid the trap of immoderate and unrealistic tests of strategic value. More specifically, the test of independent decisive effect on the course of a war is a criterion that special operations would fail in most instances. Since navies, armies, and air forces also fail the 'test' of independent decisive effect, one should not hold the special operations community to a higher standard."[17]

Similarly, an offensive cyber operation should not be considered by itself but with reference to both its direct and indirect effect upon conflict. This reveals an intricate relationship between mission excellence and strategic success. A well-written piece of code might provide great tactical value but does not guarantee strategic value, while failed usage of a cyber capability might provide strategic gains. An example of this seemingly counterintuitive logic might be Shamoon, the wiper malware that targeted the world's largest oil company, Saudi Aramco, in August of 2012.[18] The malware contained multiple coding errors and was badly executed.[19] Yet, with reference to Iran's broader conflict situation and posture in the region, it might have had a positive contribution. Not least, Iran showed it was unwilling to immediately back down following others' usage of a capability it had hardly developed at the time. The deployment showed Iran's military perseverance and perhaps even enhanced its political standing relative to other states.

The Nature of Offensive Cyber Operations

Offensive cyber operations in this article refer to computer activities to disrupt, deny, degrade, and/or destroy.[20] Offensive cyber operations generally take place across multiple stages. We commonly distinguish between reconnaissance, intrusion, privilege escalation, and payload dropping.[21] When thinking about the strategic value of offensive cyber operations, a useful distinction to consider is that of "counterforce" and "countervalue" targeting. The terms have been long used in nuclear planning as the two main courses of military action.[22] Counterforce is when an actor decides to strike at the opponent's military forces or infra-

structure. This is differentiated from countervalue strikes, which target the sources of an opponent's national strength.[23] In this context, counterforce cyber capabilities concern an offensive cyber capability designed to be used against targets relevant to the military operation. Countervalue cyber capabilities refer to an offensive cyber capability designed to be used against vital assets of the adversary. These two categories are presented as Weberian "ideal-types," meaning that in reality the distinction might become blurred.[24]

Table 1 lays out the dimensions of the two capabilities, revealing in which areas they likely overlap and differ. First, the conventional notion of "range" is not part of the definition and not a characteristic of either type of capability. Normally, range refers to the distance that a projectile may be sent by a weapon. Range is thus inherently connected to geography, a principle which has little meaning in cyberspace.[25] "Places have become geographically disembedded, that is, they are less and less determined and defined by physical-geographical features," as Philip Brey writes.[26] A capability may be counterforce even though it is used against an adversary geographically distant (but on the battlefield). And, conversely, one may attack a country nearby with a countervalue capability. There is also no inherent feature in the vulnerability, access, or payload of an offensive cyber capability that makes it either a countervalue or counterforce asset. Both capabilities can exploit software, hardware, or network vulnerabilities and can access air-gapped or non-airgapped systems. Indeed, despite some of the uncertainty about the exact vulnerability exploited in the case of Operation Orchard, it can be classified as a CFCC.[27]

The discussion on payload is associated in nuclear terminology as "yield." Also, yield is not and cannot be considered a defining feature of classifying offensive cyber capabilities. Yield is conventionally calculated using precise, physical standards. For example, it was alleged that the early Soviet intercontinental ballistic missile could carry a three megaton warhead (RDS-37) or a five megaton warhead (RDS-46).[28] A similar classification for cyber capabilities' payload is not possible; there is no convention for calculating "maliciousness" in a code as it is target dependent.[29] Having said that, for strategic purposes, as becomes clear below, it is more likely that a CFCC intends to cause less direct harm or damage than a CVCC. CVCC's principal target is the critical infrastructure of state actors. Targets may be facilities for water supply, telecommunication, electricity generation, or public health. CFCC targets military and

operational infrastructure of state and possibly nonstate actors.[30] Most nonstate actors are less dependent on territorial assets, making it more difficult to effectively use these capabilities.

Understanding the costs of these capabilities is not straightforward. Individually, a CFCC may be cheaper than a CVCC. The obstacles actors have to overcome to conduct a cyberattack against an industrial control system of a critical infrastructure are significant.[31] Yet, overall, CFCC may actually be more expensive to maintain and use, especially when these capabilities are used in response to the actions of other actors. To clarify this dynamic, imagine a situation in which there are multiple domains of potential conflict. To ensure a state actor can use counterforce capability when an adversary mobilizes its military capability in one of those domains, it must develop a capability for each domain—or at least several domains.[32] Yet, a state can use the same CVCC regardless of where the adversary will attack. The additional costs of relying on CFCC then comes from two sources: an actor needs to increase its arsenal size to impose costs on an adversary (if used reactionary), and a more constant effort to maintain the effectiveness of these capabilities is required given the transitory nature of offensive cyber capabilities.[33] This notion echoes John Lewis Gaddis's conclusion on strategies of containment.[34] A more limited form of containment, heavily relying on nuclear weapons, is cheaper but also less flexible. The more extensive form of containment—following the notion that the US would defend any territory regardless of means and area—provides more flexibility, but it also strains budgets. The aggressor chooses the location, and the receiver reacts accordingly.

Table 1. Countervalue and counterforce dimensions of offensive cyber capabilities

Dimension	CVCC	CFCC
Target	Vital asset adversary	Operationally relevant asset
Type of target	Often civilian	Often military
Range	Irrelevant	Irrelevant
Vulnerability	Undetermined	Undetermined
Access	Undetermined	Undetermined
Type of payload	Undetermined	Undetermined
Nature of adversary	Normally a state actor	Both state and nonstate actors
Costs	Individually, likely more expensive Collectively, cheaper	Individually, likely cheaper Collectively, more expensive

Numerous examples exist of counterforce targeting by state actors using offensive cyber capabilities.[35] In July and August 2008, Russia launched a DDOS-attack against Georgia's network, coinciding with troops entering the Georgian province of South Ossetia.[36] The attack, conducted in two phases, initially focused on Georgian news and government websites and later embraced a broad set of targets including educational institutions, financial institutions, businesses, and Western media.[37] The attacks complicated Georgia's efforts to manage its logistics, command forces, and deliver its war materials on time.

Another example of a CFCC is the Israeli use of the Suter Program developed by BAE systems.[38] The Israeli Air force allegedly used the technology to conduct an airstrike against a nuclear reactor in Northern Syria.[39] On 6 September 2007, F-15Is and F-16Is fighters flew into Syrian airspace, bombing the precise location of the nuclear plant in the Deir ez-Zor region of the country. Syria's air defense systems were fed a false-sky picture that allowed the Israeli fighters to conduct the entire process completely unnoticed.[40]

What are cases of CVCCs? Stuxnet can be categorized as a CVCC. Another example is the attack on the Ukraine power grid. On 23 December 2015, hackers took down almost 60 electrical substations in Ukraine, leaving more than 230,000 people without electricity for several hours.[41] As Kim Zetter writes, "They were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance."[42] Overall, there are fewer examples of countervalue cyber capabilities known today used far from national borders and fielded military forces. Herein also lies an important observation: there is still much strategic room for states to explore.

Strategic Value of Counterforce and Countervalue Cyber Capabilities

Having laid out the dimensions of CVCC and CFCC, we can now look at the distinct advantages and disadvantages of these capabilities. Four propositions emerge. The first is considered to be the "master" proposition, as the other observations follow from it.

Proposition 1: Offensive Cyber Capabilities Provide an Extra Option for State Leaders

Gray, in his review on the strategic value of special operation forces, writes:

> Special operations can expand the options available to political and military leaders. . . . In theory, there are always alternatives to the use of force—diplomacy, economic sanctions, and the like. In practice, however, there are some situations that one cannot resolve successfully without resort to physical coercion. The availability of a special operations capability means that a country can use force flexibly, minimally, and precisely. The realization by the enemy that one has a special operations capability can have beneficial effects on calculations made abroad. In time of war, both in its independent and supporting roles, special operations enhance the flexibility with which one can use force.[43]

The value of offensive cyber capabilities is very similar; having the choice to use a cyber capability expands the options available to leaders. David Sanger writes in *Confront and Conceal* that "the origins of the [US] cyberwar against Iran goes [*sic*] back to 2006, midway through George W. Bush's second term. Bush had often complained to his secretary of state, Condoleezza Rice, and his national security adviser, Stephen Hadley, that his options regarding Iran looked binary: let them get the bomb or go to war to stop it. 'I need a third option,' Bush told them repeatedly. When that option emerged, it came from inside the bowels of the US Strategic Command, which oversees the military's nuclear arsenal."[44] The product was Olympic Games. Sanger writes that the motivation behind this operation was twofold: "[t]he first was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there was a smarter, more elegant way to deal with the Iranian nuclear problem than launching an airstrike that could quickly escalate into another Middle East war, one that would send oil prices soaring and could involve all the volatile players in the region."[45]

In simple terms, it is said that offensive cyber operations allow for action within the "gray zone" of foreign activities, neither war nor peace. As scholar Herb Lin argues, "Nuclear comes AFTER conventional conflict has commenced. . . . Escalation concerns involve moving from conventional conflict to nuclear conflict. Going nuclear is escalatory. . . . [Instead,] cyber comes in the early stages of conflict (BEFORE kinetic war). In principle, cyber [is] just another weapon to be used by . . . military forces. . . . Going cyber is pre-escalatory."[46] Even though offensive cyber

operations provide an extra option, they are not the "prewar capabilities" that simply add another rung to the ladder of escalation. Offensive cyber capabilities can be used in times of both peace and war, in conflicts with different intensity, with and without kinetic force and can influence the activities of all other domains of warfare and lead to escalation or de-escalation. The exact nature and utility of usage, however, inherently differs for countervalue and counterforce capabilities, as will become clear.[47]

Proposition 2: Offensive Cyber Capabilities Can Be Used Effectively in Conjunction with Other Military Capabilities

Several scholars note that "unlike weapons of mass destruction, cyber weapons are an integral part of the commander's arsenal in conducting force-on-force and asymmetric warfare and will be used in concert with kinetic weapons to soften up the adversary's defenses."[48] Indeed, there is little question that CFCCs can be deployed in conjunction with other military capabilities—in fact, that is what makes them attractive to use. Like small amounts of investments can create much larger changes in total output of an economy through a multiplier effect, so can the use of a relatively simple CFCC greatly alter the outcome of a conflict.[49] Yet, the effectiveness of CFCCs in this manner is dependent on one key condition: force integration.

The required nature of force integration depends on the form of interdependence between the offensive cyber operations and conventional military operations.[50] First, there can be, what I call "pooled interdependence," when CFCCs and conventional capabilities perform separate functions. While the activities may not directly depend on each other, each provides individual contributions to the same goal. This is very much in line with the activities of Russia against Georgia in 2008 and more recently against Ukraine.[51] The use of multiple attack vectors caused a "mashup" of indirect dependencies leading to success of the overall engagement.

Second, there can be "sequential interdependence" when the use of a CFCC in the overall military process produces an outcome necessary for the success of subsequent conventional capability. Operation Orchard is an excellent example of how CFCCs can dramatically increase the effectiveness of other military capabilities in this manner. The F-15s and F-16s used by the Israeli air force against Syria in 2007 were not equipped with stealth technology. But tripping off Syria's air defense

radar system nevertheless ensured the Israeli air force could accomplish the missions while remaining undetected. Note that the multiplier effect may be larger for situations of sequential interdependence, yet the risks are also higher. Failed use of a CFCC may have disastrous consequences for the follow-on operation, leading to a failure of the overall process.[52]

Even though CVCCs typically are not integrated with kinetic forces on the battlefield, there are still incentives to use these capabilities in conjunction with other forces in certain conflict situations. Consider a scenario in which actor A attacks our imagined state actor (actor B) through either conventional or cyber means. The most obvious response of actor B (or ally of actor B) would be to raise the cost of the attacker (actor A) by deploying defense capabilities on the battlefield. But actor B can further raise the costs of the attack by means of using a CVCC against a vital asset of actor A. There are three conditions that could make this response particularly effective.

The first condition is perhaps the most obvious: actor B must be able to inflict enough harm or damage against actor A that it is perceived to be a substantive cost (which in turn can be leveraged). Offensive cyber capabilities that have the potential to cause high levels of harm or damage often go beyond effects created in cyberspace. One could, for instance, consider the sabotage of a water dam or power plant through a cyberattack, leading to the physical destruction of this infrastructure.

In discussions on the use of conventional capabilities for coercive purposes, the focus is generally on a geographical area. In the case of a nuclear bomb, we can calculate the different radii of serious and less serious contamination. What we cannot do is differentiate within that area. The usage of a CVCC does not come with these restrictions; its effects can be selectively dispersed across a large geographical space (e.g., all hospitals in a certain country running on a certain system). This opens up new ways of thinking when it comes to countervalue capabilities. Instead of taking down one vital asset of a country, there is also an opportunity to paralyze the country through attacking a large amount of geographically dispersed systems.

The second condition is that actor A must be able to discern with a high level of certainty that the retaliatory act through cyberspace comes from actor B. This condition might seem trivial, and it is for conventional capabilities, but for CVCCs there are two complications. First, actor A must be aware that the attack came from actor B. Plausible

deniability is normally said to be to an advantage to the attacker. Yet, in this case it is an additional hurdle for actor B, as the aim for actor B is to show that it is retaliating in response to actor A's actions. This discussion has led to early talk about the need to develop "loud" cyberweapons.[53] Second, actor A must be able to delineate actor B's cyber response from the more constant state of cyber activity. Cyberspace, given its interconnectedness, is said to be a space of constant contact, action, hostility, and change.[54] In February 2017, the director of UK's National Cyber Security Centre said that the country had experienced 188 "high-level cyber attacks" in the previous three months.[55] If allegedly a government is attacked multiple times a day by state-sponsored actors, how does it know this particular attack is part of a retaliatory strike?[56]

The third condition is that the actor designs the CVCC in such a manner that it is able to control the temporal nature of the harmful or damaging effects. Scholars often talk about the effect of offensive cyber operations only being able to be temporal.[57] But a truly intelligent design of a capability goes beyond this and aims to control the duration of effect. Control refers to the defender's inability to stop or reverse the effects of the cyberattack and the attacker's ability to stop or reverse the effects of the attack at any given time.

This type of capability design would allow for CVCC to be used somewhat similarly to economic sanctions. The simplest design for this type of capability would be large-scale DDOS attacks with multiple C2 servers and a large number of zombie computers (infected with different malware). Another type of design would be a variant of a wiper. The wiper would copy all the relevant data before it executes the disk-wiping command. The leverage is that the attacker could give the data back following conflict termination (in the scenario described above). Overall, if the usage of a CVCC is discernible and its effects controllable, it can be used as an independent asset—and even allow for the prevention of further conflict and the maintenance of stability in a certain region.[58]

In fact, countervalue cyber capabilities also have a distinct advantage compared to economic sanctions. Sanctions are inherently public, which leads to additional reputational costs for the aggressor if it backs down post-action. The value of CVCC is that these activities could potentially take place in a covert manner, making it easier for a leader to save face after it backed down. Overall, this leads to new possibilities of compellence, that is to change the behavior of actors.

Ultimately, combining the above three conditions leads to a dilemma for the use of a CVCC. After all, it is difficult to combine the first and last conditions. If an effect is created beyond cyberspace, it is hard to reverse this effect at a later time. And, the reverse is true as well: if the direct effects of an operation do remain within cyberspace, the effects may not be substantial enough to be leveraged against the opponent.

Proposition 3: Offensive Cyber Capabilities Can Be Used to Achieve a Form of Psychological Ascendancy

An extensive body of military research has been devoted to understanding the psychological impact of military operations. In particular, numerous scholars have sought to assess how the psychological effects of air operations during major conflicts—such as World War II, the Korean War, the Vietnam War, and the Persian Gulf wars—have helped to coerce and/or demoralize the adversary.[59] Also offensive cyber operations may have psychological effects. The nature of this effect, however, tends to differ from most conventional military operations: rather than frightening the adversary, the effects are subtler and relate to humiliation and confidence degradation. It is also less about threatening escalation and more about exposing vulnerability for offensive cyber operations.

An old example illustrates this particularly well. On an afternoon in June 1903, the Italian inventor and electrical engineer Guglielmo Marconi was about to demonstrate how Morse code messages could be wirelessly transmitted over long distances.[60] In the lecture theater of the Royal Academy of Sciences, Marconi's assistant John Ambrose Fleming was waiting to showcase the powerful point-to-point system technology in front of a large audience. Marconi himself was about 300 miles away, preparing to send a signal to London from a clifftop station in Cornwall, UK. Yet what followed was not in Marconi's playbook:

> Minutes before Fleming was due to receive Marconi's Morse messages from Cornwall, the hush was broken by a rhythmic ticking noise sputtering from the theatre's brass projection lantern, used to display the lecturer's slides. . . . Someone, [Fleming's assistant] Blok reasoned, was beaming powerful wireless pulses into the theatre and they were strong enough to interfere with the projector's electric arc discharge lamp. Mentally decoding the missive, Blok realized it was spelling one facetious word, over and over: "Rats." A glance at the output of the nearby Morse printer confirmed this. The incoming Morse then got more personal, mocking Marconi: "There was a young fellow of Italy, who

> diddled the public quite prettily," it trilled. Further rude epithets—opposite lines from Shakespeare—followed.[61]

A trick was played by Nevil Maskelyne, a British magician using Morse code for his illusions, enlisted by the Eastern Telegraph Company. Maskelyne's actions highlighted that Marconi's technology was nowhere near as secure as he claimed. After the incident, Marconi did not immediately respond publicly: "I will not demonstrate to any man who throws doubt upon the system." The *New Scientist* writes that, "Fleming, however, fired off a fuming letter to The Times of London. He dubbed the hack 'scientific hooliganism', and 'an outrage against the traditions of the Royal Institution'. He asked the newspaper's readers to help him find the culprit."[62]

The century-old hack aptly demonstrates a potent ability of offensive cyber operations today: the ability to humiliate an enemy. This is also demonstrated for more recent CVCC and CFCC usage. The goal of Stuxnet (a CVCC) was not to maximize damage but (in part) to embarrass the Iranians.[63] And the worm has done so successfully. Natanz was a hardened fuel enrichment plant (FEP), buried deep underground, seemingly impossible to strike. Some of the country's most renowned scientists and engineers were dismissed as incompetent, unable to explain what was going on with the industrial control systems in Natanz. The malware was only discovered after non-Iranian security researchers started to analyze the code, another sign that the Iranians were unable to protect their own most secretive and prestigious program.[64]

Operation Orchard (a CFCC) is one of the Israeli military's finest moments. For Syrian President Bashar al-Assad, it was a humiliating experience. After the attack the Syrian government initially claimed that its antiaircraft weapons had fired at Israeli fighters, which had bombed an empty area in the desert. Later, Assad insisted during an interview with *Der Spiegel* at his palace that "[t]he facility that was bombed was not a nuclear plant, but rather a conventional military installation."[65]

These types of cyberattacks remind us of the psychological effects of some of the special operations Colin Gray describes. For example, "during the war of attrition with Egypt in 1968–70, Israeli commandos attacked one of the 'crown jewels' of the Egyptian economy, the Naj Hamadi transformer station and bridge which were 320 kilometers inside Egypt. [It is an example of] a state being revealed as unable to

protect its assets."[66] Overall, both special operations and cyberattacks can "inflict exemplary punishment as well as actual loss."[67]

To achieve some form of psychological ascendancy could be both the main purpose and side effect of using an offensive cyber capability.[68] From the perspective of our imagined state actor assuming the defender and/or other third party does not disclose the intrusion, there are three options: attack and immediately disclose; attack and conceal, but disclose later; or attack and conceal. If an attacker postpones disclosure it can expose the intrusion at a time when the strategic context is more favorable (e.g. when target is particularly exposed to this news, during, for example election season, or when distraction away from internal problems is convenient). If an attacker never discloses, it can enhance credibility and make compellence easier in the future, as was stated above.

Proposition 4: Offensive Cyber Capabilities Can Be Used Effectively with Few Casualties

In 2015, when India's Prime Minster Narendra Modi launched "Digital India Week" he stated that "clouds of a bloodless war are hovering" in the world.[69] It was a reference to the global cyber threat that he believed India could play a lead role in countering.

The uses of CVCCs and CFCCs so far have indeed not been lethal, but the argument is not that it cannot happen. A civilian can be a direct and indirect target of a cyberattack. A potential example of a direct attack concerns the alteration of medical devices that could give a deadly shock if hacked. The doctor of former Vice President Dick Cheney ordered the wireless functionality of his heart implant to be disabled due to fears it might be hacked in an assassination attempt.[70] This has proven to be a valid fear following Barnaby Jack's demonstrated research on vulnerability in medical devices.[71] More indirect forms of harm can be caused by using an offensive cyber capability against transportation networks (causing airplane/train crashes) or dam facilities (causing pollution or flooding).

Instead, the notion of "bloodless war" rests on two pillars. The first pillar directly connects to the earlier debate on whether cyberwar makes for a more or less violent world. Tim Maurer concludes "cyberwarfare might be how we will fight the battles of the future. The evidence so far suggests, however, that a digital Pearl Harbor would cost fewer lives than the attack 70 years ago. It might not be pretty, but from a humanitarian

point of view, that's good news." Maurer notes that Stuxnet delayed Iran's nuclear development without killing anyone. Hence, his argument is that if actors use a Stuxnet-like capability more often, it would reduce the human costs of war.[72] Similar conceptions are provided by Thomas Rid and John Arquilla.[73]

The other pillar on which the bloodless war conception rests is that of the attacker's casualty sensitivity.[74] Though the literature is divided on whether mounting casualties by themselves drive public attitudes toward conflict and inherently lead to reduced public support, the scholarly consensus is that public attitudes toward war are not indifferent to the human costs of its soldiers.[75] The common conception is that the public makes some kind of "end-means" calculus about war.[76] A cyber warrior sits far away from the battleground—whether developing a tactical or strategic cyber capability. It is hard to conceive how these individuals can suffer bodily harm during an offensive cyber operation.[77]

Although the bloodless war perception provides a powerful push factor to use an offensive cyber capability, there is a major caveat with respect to this discussion. Offensive cyber operations can have the ability to limit casualties on both sides.[78] Yet imprudent use can severely increase the undesired impact of these capabilities. As Steve Bellovin, Susan Landau, and Herb Lin note, "indiscriminate targeting is not an inherent characteristic of all cyberattacks."[79] Historically, there has often been mismatch between the intent and the actual damage caused by cyberattacks. When graduate student Robert Morris released one of the first computer worms distributed via the internet in 1988, he never intended to create an overall system downtime leading computers to slow down to the point of being unusable. The worm's alleged purpose was to measure the size of the internet, but a critical bug in the spreading mechanism transformed it into a highly disruptive attack.

Bellovin, Landau, and Lin examine the requirements and policy implications of targeted cyberattacks.[80] Their main conclusion is that "precise targeting requires good technical design . . . [and] intelligence . . . of the target's environment."[81] The scholars indicate that precise intelligence on the configuration of target machines is especially important when cyberattacks focus on physical assets, considering the high risk of collateral damage.[82]

What should also be noted is that, as discussed for Proposition 2, the relationship between spatial area of damage and collateral damage is

more complex for CVCCs compared to the use of conventional capabilities. There does not have to be any correlation between the geographical distribution of effects and the distinctive or targeted nature of an offensive cyber operation. Overall, the belief held in many military quarters is that with sufficient testing and retesting prior to usage, offensive cyber operations can achieve a designed effect and minimize damage to entities that should remain unharmed.[83] But it does mean that the costs for developing an offensive cyber capability are substantially higher too.

Conclusion

This article examined the strategic value of offensive cyber operations, distinguishing between counterforce and countervalue cyber capabilities. While distinct advantages exist for using offensive cyber operations, it should be clear that there are many things offensive cyber operations cannot do. The cyber warrior is much more anonymous, and the way cyber operations unfold will not create the kind of heroics that raise public morale. At the same time, the effective use of offensive cyber capabilities comes with a number of conditions that can sometimes be difficult to meet and might even conflict. A better conceptualization of these conditions and potential trade-offs helps set the required technical parameters of future cyber capability development.

Ultimately, offensive cyber operations can lead to significant strategic advantages for a state actor. They can serve as a force multiplier as well as an independent strategic asset. Above all, the potential use of offensive cyber capabilities provides an extra option to state leaders across a range of situations. SSQ

Notes

1. Quoted in Mike Levine, "Russia Tops List of 100 Countries that Could Launch Cyberattacks on US," ABC News (18 May 2017), http://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188.

2. Jamie Shea, "Lecture 6—Cyberattacks: Hype or an Increasing Headache for Open Societies?" (transcript, 29 February 2012), http://www.nato.int/cps/en/natolive/opinions_84768.htm; and INFOSEC, "The Rise of Cyber Weapons and Relative Impact on Cyberspace," Infosec Institute, (5 October 2012), http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/.

3. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401–28, https://

doi.org/10.1080/01402390.2012.663252; and Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Brace and Company, 1946).

4. The post-2000 literature's primary focus has been on the disruptive or destructive effects of cyberattacks. The mainstream debate on the potential for cyberwar is notably illustrative. An often-cited quote from Thomas Rid's article "Cyber War Will Not Take Place" reads, "no cyber offense has ever injured a person. No cyber attack has ever damaged a building." The statement has been debated repetitively and at length, from both theoretical and empirical perspectives. John Stone writes in a theory-driven response to Rid's article that cyberattacks could constitute acts of war, but "it depends on the meaning and relationship of the terms 'force,' 'violence,' and 'lethality.' " From an empirical perspective, scholars have criticized Rid because many of the attacks cited were in fact much more violent. Perhaps not the direct effects but the indirect effects of the DDOS attacks on Estonia, one scholar argues, were consequential. Similarly, others have argued that Stuxnet was more than just an act of sabotage. *See* Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, http://doi.org/b4fkhh; John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (2013): 101–8, http://doi.org/cp6d. For direct discussions on this quote, see, for example, Gary McGraw, "Cyber War Is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies* 36, no. 1 (2013): 109–19, http://doi.org/cp6f; Isabelle Duyvesteyn, "Between Doomsday and Dismissal: Cyber War, the Parameters of War, and Collective Defense," Atlantische Commissie (2012), accessed 23 May 2018, https://www.atlcom.nl/ap_archive/pdf/AP%202014%20nr.%207/Duyvesteyn.pdf; Shruti Tulpule, "Are We Headed towards Web War I?," *International Journal of Law and Legal Jurisprudence Studies* 1, no. 7 (2014), accessed 23 May 2018, http://ijlljs.in/wp-content/uploads/2014/11/Are-we-headed-towards-Web-War-I-Shruti-Tulpule.pdf; on Estonia and student, see "Stuxnet: Computer Worm Opens New Era of Warfare," *60 Minutes*, CBS News (4 March 2012), transcript, https://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/; Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 57–64, http://doi.org/bm7g9s.

5. Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History* (London: Penguin Books Limited, 2014), 334.

6. Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Random House, 2016).

7. Cited in Patrick Cirenza, "The Flawed Analogy between Nuclear and Cyber Deterrence," *Bulletin of the Atomic Scientists* (22 February 2016), http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179.

8. *See* Max Smeets, "What It Takes to Develop a Cyber Weapon: Nobody Knows," Council on Foreign Relations: Net Politics, 21 November 2016, https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows; and Herbert Lin, "Oft-Neglected Cost Drivers of Cyber Weapons," Council on Foreign Relations: Net Politics, 14 December 2016, https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons.

9. In reality, of course, the defender has a great deal of agency in terms of the outcome of a cyberattack.

10. Thus far, the literature is divided on whether the threat of using a cyber capability can coerce. Christopher Whyte, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy* 35, no. 2 (2016): 93–102, http://doi.org/cp6g; Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony," *Journal of Strategic Studies* 40, no. 7 (2017): 1–29, http://doi.org/cp6h; Erica D.

Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (May 2017): 452–81, http://doi.org/cp6j; Richard J. Harknett, "Article Review 84 on 'The Logic of Coercion in Cyberspace' and on 'Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony,' " International Security Studies Forum, 26 September 2017, https://issforum.org/articlereviews/84-cyber.

11. For an overview of strategies, see Robert J. Art, "To What Ends Military Power?," *International Security* 4, no. 4 (1980): 3–35, http://doi.org/cjgtvg.

12. Indeed, opinions range from "leave it—it's working," to "tweak it and it'll work," to "get rid of it and start thinking about other strategies." At the same time, the table also shows much overlap in viewpoints on cyber deterrence, which often goes unacknowledged.

13. There is also disagreement on the meaning of the term "cyber deterrence."

14. I adopt the definition used by Colin Gray with two alterations. Gray looks at "how a military directly contributes to the strategic outcome of a war." First, the effects can be direct as well as indirect. Second, strategy can relate to a broader context than "war." I therefore refer to "conflict" instead. Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger Publishers, 1996).

15. Erik Gartkze, "The Myth of Cyberwar," *International Security* 38, no. 2 (Fall 2013): 42, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.

16. I avoid using the term "strategic utility" as the modern use of the term is associated with economic cost-benefit analysis.

17. Gray, *Explorations in Strategy*, 166.

18. Lucian Constantin, "Kill Timer Found in Shamoon Malware Suggests Possible Connection to Saudi Aramco Attack," *Computerworld*, 23 August 2012, http://www.computerworld.com/article/2491501/malware-vulnerabilities/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html.

19. Dmitry Tarakanov, "Shamoon the Wiper: Further Details (Part II)," SecureList, 11 September 2012, https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/.

20. A common distinction is made between three types of computer network operations (CNO): computer network defense (CND), which is protecting your own networks from being attacked or exploited; computer network exploration (CNE), which refers to computer espionage; and computer network attack (CNA), which concerns cyber activities to disrupt, deny, degrade, and/or destroy. I focus on the latter type of activity, which I term offensive cyber operations. This also means that this research does not focus on information weapons or disinformation campaigns.

21. For more information, see Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks," *Proceedings of the 9th International Conference on Cyber Conflict, Defending the Core*, ed. H. Roigas, R. Jakchis, L. Lindstrom, T. Minarik (Tallinn, Estonia: NATO CCD COE Publications, 2017), http://doi.org/cp7w.

22. Dieter S. Lutz, "A Counterforce/Countervalue Scenario—or How Much Destructive Capability is Enough?," *Journal of Peace Research* 20, no. 1 (1983): 17–26, http://doi.org/ckgb7t.

23. William A. Stewart, "Counterforce, Damage-Limiting, and Deterrence," RAND Corporation, July 1967, accessed 24 May 2018, https://www.rand.org/content/dam/rand/pubs/papers/2008/P3385.pdf.

24. Austin Long has previously made a similar distinction. However, the scholar does not go into detail on the strategic advantages of each capability. *See* Long, "A Cyber SIOP? Operational Consideration for Strategic Offensive Cyber Planning," *Journal of Cybersecurity* 3, no. 1 (2017): 19–28, https://doi.org/10.1093/cybsec/tyw016.

25. This does not mean that geography and borders do not matter at all in cyberspace.

26. Philip Brey, "'Space-Shaping Technologies and the Geographical Disembedding of Place," in *Philosophy & Geography vol. III: Philosophies of Place*, ed. A. Light and J. M. Smith (New York: Rowman & Littlefield, 1998), 239.

27. *See* Adlee's discussion on the possibility of backdoors. Sally Adlee, "The Hunt for the Kill Switch," IEEE Spectrum, 1 May 2008, https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

28. John Pike, Charles Vick, Mirko Jacubowski, and Patrick Garrett, "R-7/SS-6 SAPWOOD," Federation of American Scientists, 29 July 2000, https://fas.org/nuke/guide/russia/icbm/r-7.htm.

29. For similar points, see Michael Fischerkeller, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies," *Survival* 59, no. 1 (2017): 103–34, http://doi.org/cp7z.

30. Notice that in practice, operational infrastructure and critical infrastructure may overlap. For example, the distinction becomes blurred if one takes down the electricity grid that feeds a town and a military base.

31. More research should be conducted to better understand these costs dynamics. For an initial discussion see Max Smeets, "What It Takes to Develop a Cyber Weapon" (working paper, Columbia School of International and Public Affairs Tech & Policy Initiative, Working Paper Series 1, 2016), 49–67, https://sipa.columbia.edu/sites/default/files/WorkingPaperSeries_1.pdf.

32. This depends on the overlap in weaknesses to exploit.

33. Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1–2 (2018): 6–32, http://doi.org/cp75.

34. John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (Oxford, UK: Oxford University Press: 1982).

35. One may consider counterforce operations also in a broader sense, that is, those operations that did not cause any harm or damage. An interesting case of this kind concerns a variant of X-Agent malware for Android devices created by Fancy Bear to collect intelligence on Ukrainian field artillery units. A Ukrainian officer had developed an app to simplify artillery troops' targeting data for the D-30 towed howitzer. See Crowdstrike Global Intelligence Team, "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," Crowdstrike, 23 March 2017, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

36. Asmus Ronald, *Little War that Changed the World: Georgia, Russia and the Future of the West* (New York: Palgrave Macmillan, 2010); and Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* 91, no. 6 (November–December 2011): 63–64, https://www.questia.com/library/journal/1G1-273195159/the-2008-russian-cyber-campaign-against-georgia.

37. Numerous patriotic hackers are said to have joined the campaign in the second phase.

38. A good overview of this capability is provided by Zheng. Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," trans. Yang Fan, in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford, UK: Oxford University Press, 2015).

39. David A. Fulghum, Robert Wall, and Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology*, 26 November 2007, 28–31, http://archive.aviationweek.com/issue/20071126; Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Harper Collins, 2010); and Zheng, "From Cyberwarfare to Cybersecurity."

40. Although most scholars and media sources have looked at the event in 2007, it can be said that first part of this operation started much earlier. As *Der Spiegel* reports:

> [i]n late 2006, Israeli military intelligence decided to ask the British for their opinion. But almost at the same time as the delegation from Tel Aviv was arriving in London, a senior Syrian government official checked into a hotel in the exclusive London neighborhood of Kensington. He was under Mossad surveillance and turned out to be incredibly careless, leaving his computer in his hotel room when he went out. Israeli agents took the opportunity to install a so-called "Trojan horse" program, which can be used to secretly steal data, onto the Syrian's laptop. The hard drive contained construction plans, letters and hundreds of photos. The photos, which were particularly revealing, showed the Al Kibar complex at various stages in its development. At the beginning—probably in 2002, although the material was undated—the construction site looked like a treehouse on stilts, complete with suspicious-looking pipes leading to a pumping station at the Euphrates.

See Erich Follath and Holger Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel*, 2 November 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-2.html.

41. Initially, 30 substations were taken down. The attackers later targeted two other power distribution centers. For overviews, see Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *Wired*, 20 January 2016, https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/; Kaspersky Lab, "BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents," SecureList, 28 January 2016, https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents /73440/; and Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

42. Zetter, "Inside the Cunning, Unprecedented Hack."

43. Gray, *Explorations in Strategy*, 174.

44. David E. Sanger, *Confront and Conceal* (Portland, OR: Broadway Books, 2012), 190–91.

45. Sanger, *Confront and Conceal*.

46. Herb Lin, "Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers" (presentation, Hoover Institution / Center for International Security and Cooperation, Stanford University, CA, 15 May 2015), https://sipa.columbia.edu/sites/default/files/Thinking%20about%20Nuclear%20and%20Cyber%20Conflict-Columbia-2015-05-14.pdf.

47. Kinetic warfare "involve[s] the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles." US Air Force, "Air Force Glossary: Doctrine Document 1-2," 11 January 2007, http://www.globalsecurity.org/military/library/policy/usaf/afdd/1-2/afdd1-2-2007.pdf.

48. James Bret Michael, Eneken Tikk, Peter Wahlgren, and Thomas C. Wingfield, "From Chaos to Collective Defense," *Computer* 43, no. 8 (August 2010): 91–94, http://doi.ieeecomputersociety.org/10.1109/MC.2010.228; and US Department of Defense (DOD), Quadrennial Defense Review Report (Washington, DC: DOD, February 2010) https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf.

49. However, whereas the multiplier effect in economics takes time to work—often, several months pass before some of the effects are felt—this is not the case for offensive cyber operations, where (expected and desired) multiplier effects tend to take place over the course of days, or shorter. Also, this notion of CFCC as a force multiplier has led to the view that "cyber" is a key dimension of modern hybrid warfare. Frank Hoffman writes that "[h]ybrid wars are not new, but they are different. In this kind of warfare, forces become blurred into the same

force or are applied in the same battlespace." Sorin Dumitru Ducaru, "The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO," *Europolity* 10, no. 1 (2016): 7–23, http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf; James N. Mattis and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Warfare," *Naval Institute Proceedings* 131, no. 11 (November 2005): 30–32, https://www.usni.org/magazines/proceedings/2005-11/future-warfare-rise-hybrid-wars. For a more elaborate discussion also see Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies, 2007).

50. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (London: Transaction Publishers, 1967). These categories are adapted from Thompson's work on interactions and behaviors within an organizational structure.

51. A report from the UK House of Commons states "[a] recurring theme in Russian military strategy is the ability to combine tools seamlessly, to give a fully integrated, comprehensive approach. The Russian attitude to cyber as a tool for warfare is no different, with a full-spectrum approach integral to the strategy of the Russian Government." The use of the word "seamless" might be misleading considering Russia's conscious ongoing efforts to develop this approach, learning from its mistakes along the way. Indeed, Russia's attack on Georgia in 2008 was only partially successful, yet the more recent attacks on Ukraine suggests that it studied the lessons learned. Defense Committee, UK Parliament, "Russia: Implications for UK Defence and Security," House of Commons, 30 June 2016, https://www.publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/10710.htm; and David J. Smith, "How Russia Harnesses Cyberwarfare," *Defense Dossier* 4 (August 2012): 7–11, http://www.afpc.org/files/august2012.pdf.

52. This is in many ways similar to the industrial process of product-line development. Ironically, this also leads to the conclusion that, although integration is necessary, more integration is not necessary better.

53. The discussion of "loud cyber weapons" has primarily been about deterring future intrusions. Yet, it should also be considered in light of mitigating current intrusions and conflict. Quote from Chris Bing, "U.S. Cyber Command Director: We Want 'Loud,' Offensive Cyber Tools," FedScoop, 3 August 2016, https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016; Herb Lin, "Developing 'Loud' Cyber Weapons," *Lawfare* (blog), 1 September 2016, https://www.lawfareblog.com/developing-loud-cyber-weapons; Herb Lin, "Still More on Loud Cyber Weapons," *Lawfare* (blog), 19 October 2016, https://www.lawfareblog.com/still-more-loud-cyber-weapons; Adam Segal, "Takeaways From a Trip to the National Security Agency," *NetPolitics* (blog), 21 December 2016, https://www.cfr.org/blog-post/takeaways-trip-national-security-agency; and Timothy M. Goines, "Overcoming the Cyber Weapons Paradox," *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): 86–111, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Goines.pdf.

54. Richard J. Harknett and Michael P. Fischerkeller, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93, http://doi.org/cp9b.

55. Quoted in Nick Ismail, "Under Attack: The UK Exposed to Constant Hostile Cyber Threats," Information Age, 13 February 2017, http://www.information-age.com/uk-constant-threats-cyber-attacks-123464417/.

56. For high-level counterforce cyber retaliation, it might nevertheless be possible, but if retaliation is used on a smaller scale it will be substantially more difficult.

57. According to Gartzke, this dimension is a key limitation: "Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable

harm on an adversary." The argument here is that cyberattacks can be turned into a strategic advantage as well. *See* Gartzke, "Myth of Cyberwar," 43.

58. There are, however, a set issues which have not been well-considered. For example, even if an effect is reversible, the targeted actor is likely to have lost general confidence in the integrity of the systems.

59. The effectiveness of these campaigns remains contested. *See* E. B. Strauss, "The Psychological Effects of Bombing," *Royal United Services Institution Journal* 84, no. 534 (1939): 269–82, http://doi.org/djj3h3; Stephen T. Hosmer, "Psychological Effects of U.S. Air Operations in Four Wars, 1941–1991: Lessons for U.S. Commanders," RAND Monograph Report RB-38 (Santa Monica, CA: RAND Corporation, 1998), https://www.rand.org/pubs/monograph_reports/MR576.html; and Martin Obschonka, Michael Stuetzer, P. Jason Rentfrow, Jeff Potter, Samuel D. Gosling, "Did Strategic Bombing in the Second World War Lead to 'German Angst'? A Large-Scale Empirical Test across 89 German Cities," *European Journal of Personality* 31, no. 3 (2017): 234–57, http://doi.org/cp9d.

60. Paul Marks, "Dot-Dash-Diss: The Gentleman Hacker's 1903 lulz," *New Scientist*, 20 December 2011, https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/?full=true. Telegraphy companies had invested in a dense network of land and sea cable network. The transatlantic wireless messaging service was a major threat to their competitive position.

61. Marks, "Dot-Dash-Diss."

62. Marks.

63. Sanger, *Confront and Conceal*, 199.

64. The worm was found by Sergey Ulasen in 2010 from VirusBlokAda, a relatively unknown security firm in Belarus. The worm was subsequently analyzed by researchers from Symantec, the Langner Group, and, later, others. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, 7 November 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

65. *Der Spiegel*, "S*piegel* Interview with Syrian President Bashar Assad: 'Peace without Syria Is Unthinkable,'" *Spiegel* Online, 19 January 2009, http://www.spiegel.de/international/world/spiegel-interview-with-syrian-president-bashar-assad-peace-without-syria-is-unthinkable-a-602110.html.

66. Gray, *Explorations in Strategy*, 178.

67. Gray, 178.

68. Many talk about the reputation damage a company suffers after it falls victim of a successful cyberattack. For a major cyber incident—like those experienced by Target, J. P. Morgan, Ashley Madison, or Sony Pictures Entertainment—a company is said to face significant financial consequences (and management shake-ups). These reputation costs are often much higher than the cost to replace or restore the computer network that was initially damaged by the attack. (While companies normally suffer a drop in stock value directly after the breach/hack, stock prices normally quickly bounce back up. But the company suffers other breach/hack-related costs—also often including lawsuits.) Though governments might not run a "reputation risk" when their systems get compromised, which is quantifiable in company losses, successful compromise by an adversary can reduce general public trust authority (or factions which are responsible for a specific program)—which in turn can be exploited by other states. *See* Elena Kyochko and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, 31 March 2015, https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

69. Quoted in PTI, "World Facing 'Bloodless' Cyber War Threat: Modi," *The Hindu*, 1 April 2016, http://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece.

70. Sanjay Gupta, "Dick Cheney's Heart," *60 Minutes*, CBS News, 20 October 2013, http://www.cbsnews.com/news/dick-cheneys-heart/; Andrea Peterson, "Yes, Terrorists Could Have Hacked Dick Cheney's Heart," *Washington Post*, 21 October 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.ea14d571e5fc.

71. William Alexander, "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode," VICE, 25 June 2013, https://www.vice.com/en_se/article/i-worked-out-how-to-remotely-weaponise-a-pacemaker. In 2012, Jack demonstrated how a model of an insulin pump could be lethally hacked to administer incorrect dosages from up to almost 100 meters away. In 2013, he hacked into a pacemaker to show he was able to explode it.

72. Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, 19 October 2011, http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/. Maurer considers a scenario in the past in which former Vice President Dick Cheney describes the decision-making process that occurred as the US considered whether or not to bomb a Syrian nuclear facility in 2007. Despite Israeli requests to do so, President George W. Bush decided to pursue a diplomatic rather than military option. So Israel took matters into its own hands. Cheney writes, "[u]nder cover of darkness on September 6, 2007, Israeli F-15s crossed into Syrian airspace and within minutes were over the target at al-Kibar. Satellite photos afterward showed that the Israeli pilots hit their target perfectly." (Quoted in Maurer, "Case for Cyberwarfare.") For Maurer, this highlights an important point: "Despite the attack being a perfect hit, a few people were probably still killed." (ibid.)

73. Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016). Libicki does not buy into the "peaceful nature thesis" as it only holds in a few theoretical scenarios. Libicki does not contest that cyberattacks have the potential to cause fewer casualties as the alternative is less often chosen than others conceive it to be. The key question here seems to be whether cyber capabilities are used instead of war or doing nothing. Most examples cited by proponents of the "peaceful nature" argument focus on when a state could have gone to war but used a cyber capability instead. The Iranian attack against Saudi-Aramco and the North Korean attack against Sony may be two cases that follow the reverse pattern; instead of doing nothing, a cyberattack was conducted.

74. Christopher Gelpi, Peter D. Feaver, and Jason Reifler, *Paying the Human Costs of War: American Public Opinion and Casualties in Military Conflicts* (Princeton, NJ: Princeton University Press, 2009).

75. For an excellent overview see Christopher Gelpi, Peter D. Feaver, and Jason Reifler, "Success Matters: Casualty Sensitivity and the War in Iraq," *International Security* 30, no. 3 (2005–2006): 7–46, https://www.belfercenter.org/publication/success-matters-casualty-sensitivity-and-war-iraq; and Peter D. Feaver and Christopher Gelpi, *Choosing Your Battles: American Civil-Military Relations and the Use of Force* (Princeton, NJ: Princeton University Press, 2004).

76. Bruce Jentleson, "The Pretty Prudent Public: Post-Vietnam American Opinion on the Use of Military Force," *International Studies Quarterly* 36, no. 1 (March 1992): 49–74, https://www.jstor.org/stable/2600916; Rebecca L. Britton and Bruce Jentleson, "Still Pretty Prudent," *Journal of Conflict Resolution* 42, no. 4 (1998): 395–417, https://www.jstor.org/stable/174436; Eric Larson, *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations* (Santa Monica, CA: RAND, 1996); Steven Kull, "What the Public Knows That Washington Doesn't," *Foreign Policy*, no. 101 (Winter 1995–1996):

102–15, https://www.jstor.org/stable/1149411; and Peter Feaver and Christopher Gelpi, "How Many Deaths Are Acceptable? A Surprising Answer," *Washington Post*, 7 November 1999, http://www.washingtonpost.com/wp-srv/WPcap/1999-11/07/061r-110799-idx.html. Several factors are listed in the literature as to what can shape this calculus. Jentleson's "pretty prudent" public argument is that tolerance is based on the objective of the military operation. Larson argues that tolerance depends on "elite consensus" behind the mission. Kull believes that the international support for a mission is the essential factor. And Feaver and Gelpi identify expectation of success as a key factor of explaining public casualty tolerance.

77. Interestingly, this conclusion was also drawn in an article written by a senior National Security Agency official, William Black, in 1997. Black states, "Another aspect of warfare that came with the Information Age is that actual, physical combat be viewed in living rooms of America via television. The horrors of war cannot be hidden. As a result, in the simplest of terms, 'body bags' are no longer acceptable. There is considerable societal pressure to find non-lethal means of accomplishing tasks that once called for conventional military action." William B. Black, "Thinking Out Loud About Cyberspace," *Cryptolog* 23, no. 1 (Spring 1997): 1–4, https://nsarchive2.gwu.edu//dc.html?doc=2700088-Document-11.

78. Thomas Rid, *Rise of the Machines*: *A Cybernetic History* (New York: W. W. Norton, 2016). As Rid writes in chapter 7, *Omni* was one of the first magazines depicting the changing nature of war in 1979. Talking about the future of cybernetic war, *Omni* envisioned four features: speed, automation, espionage, and precision.

79. Steve Bellovin, Susan Landau, and Herb Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3, no. 1 (March 2017): 59–68, https://doi.org/10.1093/cybsec/tyx001.

80. There is nothing inherent to either CVCC or CFCC that makes one or the other more likely to cause undesired impact.

81. Bellovin, Landau, and Lin, "Limiting the Undesired Impact," 59.

82. Bellovin, Landau, and Lin, 59.

83. Bellovin, Landau, and Lin, 59. The main argument of Bellovin, Landau, and Lin's article is that precise targeting requires a "good technical design" and "good intelligence." At minimum, this conclusion is unspecified, as it is unclear what "good" means. A potentially more severe critique is that the empirical cases cited do not support the authors' conclusions. The scholars consider the DDOS attacks on Estonia and Georgia as two cases in which cyber-attacks were discriminate. Analysis of both these cases suggests, however, the technical and intelligence requirements were rather limited.