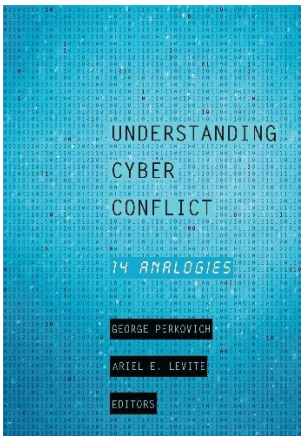
Conclusions

George Perkovich and Ariel E. Levite

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



For additional information about the book:

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

Conclusions

GEORGE PERKOVICH AND ARIEL E. LEVITE

International society and governments are only beginning to understand the attributes of cyber capabilities and the possible nature of cyber conflicts. A principal value of analogies is to clarify which features of cyber capabilities and potential conflict are most pertinent to analyze and understand and which are less relevant or important to preventing conflict and to conducting cyber operations. Analogies help sharpen questions and identify dilemmas.

Readers may disagree, of course, with the observations we make here. Debate is welcome. One of the attractions of analogies is that, like art, they elicit the perspectives, experiences, and outlooks of the beholder. This invites conversation or debate among observers in which all parties may gain by appreciating a new angle, by affirming or discarding a prior assumption, by seeing or learning something entirely new. Our conclusions here are offered in this spirit. We have resisted the temptation to make policy recommendations for the US or other governments. Some of the foregoing chapters imply or suggest steps that governments could take to avert or minimize dangers of cyber conflicts, but as a general proposition we find that the cyber world is evolving so fast, with so many complicating factors (as we describe in the following sections), that policy prescriptions not made in context and in real time would be suboptimal. However, we do offer general principles and objectives later in this conclusion for policymakers to consider.

What Are Cyber Weapons Like (Not Like)?

Drawing on all the chapters in this volume, here we attempt to summarize the defining characteristics of cyber weapons and, where helpful, how they differ from other military technologies.

Distinct, Essential Qualities of Cyber Capabilities

Information and communication technology (ICT), hereafter referred to as cyber technology, is dual use in the sense of serving benign and malign purposes. No previous dual-use technology has so thoroughly and quickly produced both peaceful and hostile applications on a global scale as cyber technology has.

Aircraft, railways, telegraph, and radio dramatically augmented civilian life, including commerce, while also boosting military potency. But the combined pace and scale of dual-use cyber technologies' dispersion and impact are unique. The growing dependence on cyber in many facets of modern life, including the Internet of things, makes managing vulnerabilities to disruption extremely challenging. We discuss implications of this in the second and third sections of this conclusion.

Cyber capabilities also are uniquely protean as instruments of intelligence gathering and coercion. The same basic tools and operators can be utilized in multiple ways to achieve a wide range of objectives. The range includes intelligence collection, political-psychological warfare, deterrence signaling, discrete sabotage, combined-arms military attacks, and campaigns of mass disruption. Other technologies also can be effective to achieve each of these objectives. Burglars could penetrate a political party's headquarters and steal and then publish sensitive files, though probably not as fulsomely as can be done by cyberespionage and by disseminating exfiltrated information via social media. Radio can transmit propaganda and other subversive information, just as the Internet does. Aircraft can drop laser-guided bombs to destroy a nascent weapons-plutonium production capability, as they did in Syria in 2007. But no other type of technology can be utilized in such diverse ways as cyber technology.

The versatility and ubiquity of cyber capabilities greatly enhance their appeal for intelligence collection, military operations, covert actions, and clandestine signaling. For powerful states, cyber can be a substitute, a precursor, and a complement to classic operations. For other actors—state and non-state—who find themselves in highly competitive security environments with technically sophisticated adversaries, cyber instruments may be uniquely attractive as power balancers.

The benefits of versatility are magnified by the relative ease of entry into the offensive cyber world. Compared to advanced kinetic and nuclear weapons and platforms, and their related reconnaissance and battle management capabilities, cyber capabilities are compellingly affordable. It is much easier and cheaper to recruit and train personnel to develop and operate cyber capabilities than it is to develop an effective conventional, nuclear, or biological war-fighting capability. For states that cannot develop their own cyber capabilities and cadres, these "goods" and services can be procured readily in the gray and black markets. The low barrier to entry is another important way in which cyber capabilities are unlike most other weapon technologies and why so many diverse actors can compete in this domain.

Still, turning cyber capabilities into effective and dependable weapons—as distinct from criminal tools and terror weapons—presents formidable challenges. In military and covert operations, the ability to ascertain impact and tailor effects is critical both to build confidence that intended results would be achieved and to avoid collateral damage and unintended secondary and tertiary consequences; however, the effects of cyber weapons may be uncertain and therefore difficult to predict with confidence. Cyber weapons may be viable only for short or at least uncertain amounts of time. Maintaining their effectiveness

in the face of routine systems maintenance or specific defensive countermeasures is time and resource consuming. Constant monitoring of targeted networks is required.

Assuming concerns over the uncertainty of effects and durability can be mitigated, another distinct and attractive feature of cyber capabilities—for espionage and attack—is their stand-off potential. They can be operated from a distance to achieve global reach, sparing the conductors from friction with intermediaries and from risks of interdiction, capture, or death. (Satellites are similar in this regard, though they differ in that they are more difficult and expensive to build and deploy and do not directly carry out attacks.) The personnel protection afforded by cyber capabilities reduces the risk that an agent or soldier will be captured and used to create a spectacle that can escalate the intruded-on state's determination to retaliate and, in turn, create pressure on the captured asset's government either to escalate or to bargain to obtain his or her release. The worldwide range of cyber capabilities makes them especially attractive to states (and criminals) that cannot otherwise reach targets. For states that do have other long-range strike capabilities, the relatively low cost and personnel risks of cyber attack may be preferable. These effects cut multiple ways: they open not only a wide potential of offensive operations but also a similarly vast vulnerability to being attacked by cyber weapons from anywhere.

Cyber capabilities can be uniquely secretive, only partly due to the distances and conduits through which they can be operated. The development, the deployment, and often even the use of cyber assets are not easily observable—unlike air bases, naval forces, and drones. Secrecy provides operational advantages for intelligence gathering, covert operations, and war fighting. The low visibility of (some) cyber operations also allows potential victims to choose whether to publicize them. This creates political space for them to save face if they choose not to retaliate.

Seen from a different angle, the imperative to keep capabilities and, in most cases, operations secret makes it less likely that governments, let alone citizenries, will conduct informed debates over whether, when, and how (1) to conduct offensive cyber operations and (2) to develop effective international norms and rules for such operations. We discuss this implication further in the third section of this chapter.

Secrecy facilitates and is augmented by the distinct difficulty of confidently attributing the precise origin of attack and who actually is responsible for authorizing it. A precision-guided missile (PGM) or bomber can be readily and confidently traced to its source. Chemical explosives used in terrorist or covert operations also can often be traced to their sources, albeit with ambiguity about whether a particular state sponsored the attack. In the case of cyber weapons, the multitude of possible attackers, the potential concealment or falsification of attackers' identities, the diversity of effects, and the globally distributed vectors of attack make determining the authorial source of an observed effect difficult and time consuming. It is especially daunting to attribute cyber penetrations and attacks with the speed, resolution, and confidence needed to enable states to

decide on, publicly justify, and tailor punitive responses. Forensic analysis alone rarely enables sure attribution; other sources and methods are often necessary. But states are reluctant to reveal these means, thus further complicating the challenges of attribution and the viability of deterrence by punishment.

The attribution problem may be less pressing in the context of overt warfare when combatants will reasonably presume that cyber attacks are coming from the same source as other forms of attack and the risk of misidentification may be modest. However, in covert contests short of armed conflict, attribution will complicate when and how antagonists interpret and respond to attacks. We discuss these challenges further later.

Cyber Effects and Their Implications

Turning now to specific functions, Michael Warner describes in chapter 1 how modern information and communications technologies have greatly enhanced states' and other actors' capacities to gather and analyze intelligence and to conduct covert operations. The advent of the telegraph and radio in the nineteenth and twentieth centuries also enhanced intelligence collection and guidance of military operations in radical ways. But these enhancements were not nearly as swift, widely distributed, and powerful as those provided by cyber. The dispersal of information and communications technologies and networks means that "anyone with a network connection can be a victim of espionage mounted from nearly anywhere." The growing availability of techniques to overcome the so-called air gap, and thereby siphon information from ICTs that are unconnected to the Internet, extends vulnerability. Both developments are new.

A major distinction between cyber capabilities and other technologies, including radio and satellites, is that the software and operations deployed to gather intelligence by cyber means also can be readily and directly used to conduct attacks. Satellites and related communications technologies must be linked both to physical delivery means such as missiles, planes, ships, and other platforms and to payloads to conduct attacks. By contrast, the same cyber tool and operation used to exfiltrate information also can be used as precursors as well as platforms for attack, even if some capabilities (especially payloads) would need to be added to fully weaponize them.

It is possible that intelligence gathering, if discovered by the target, could instigate a crisis or escalate a conflict. Yet, experience to date, albeit limited, suggests that states understand that cyber intelligence gathering is to be expected and managed without recourse to war, as is the historical norm. For example, Edward Snowden's revelations of US cyber intelligence gathering did not prompt targeted states to initiate conflict. Nor did the discovery that China had penetrated and exfiltrated massive amounts of data from US government files and health insurance providers cause the United States to take classical military action.

It is also possible that rather than cause conflict, the discovery of deep cyber penetration of a system, especially when it is air gapped (i.e., never connected to the Internet), may cause the penetrated state to reconsider the conduct of illicit

or otherwise threatening activity. Some observers believe, for example, that the Stuxnet operation motivated Iran to accept constraints on its nuclear program, not because roughly a thousand centrifuges were damaged, but because the cyber penetration of the enrichment program alarmed Iranian leaders that they could not maintain the secrecy required to complete the development of nuclear weapons.

New challenges do arise from the proven potential of cyberespionage tools to become precursors as well as instruments of attack. If and when adversaries—say, the United States and Russia or China—are embroiled in a crisis and have increased the deployments and readiness of their military forces, the discovery of a cyber penetration into one's command-and-control systems and/or nuclear early warning systems could be unnerving and destabilizing. The state that conducted the penetration may be intending only to gather intelligence and early warning, and perhaps to communicate a deterrent signal, but the penetrated state may perceive the penetration as a harbinger of attack. Depending on the circumstances and the vulnerability that the penetrated state feels to preemptive attack, pressures could grow on that state to use its forces while it still can. Furthermore, the tight compartmentalization that intelligence organizations customarily impose on sensitive sources and methods, such as when monitoring adversary strategic command-and-control systems, greatly exacerbates the potential for cyber espionage to trigger inadvertent escalation. Clearly, the nature of cyber intelligence-gathering technology has uncharted implications for the potential conduct of cyber war and for efforts to prevent or manage it.

Moving from intelligence gathering to coercion, cyber weapons are especially—perhaps uniquely—useful in the gray zone of confrontation below armed conflict. The Russians' 2007 cyber attacks on Estonia, the US-led Stuxnet attack on Iranian centrifuges, the Iranians' destructive 2012 attack on Saudi Aramco's desktop computers and 2011–13 denial of service attacks on US banks, and the 2014 North Korean attack on Sony Pictures Entertainment—all exemplify diverse secretive coercive cyber operations short of warfare.

That said, cyber capabilities also create effects that can be vital to the conduct of war (and terrorism). Cyber capabilities now indispensably enable most of the communications, reconnaissance, command-and-control, and operational functions of modern militaries. Cyber networks do more for militaries than any other single previous technology, greatly boosting the defensive and offensive capacity of states and their militaries. At the same time, of course, it also makes them vulnerable to disruption in unprecedented ways.

Complementing their enabling potential, cyber weapons also can be disruptive or destructive in and of themselves. Like earlier forms of electronic warfare, they can blind, deceive, degrade, and even disable and destroy an opponent's communications, reconnaissance systems, navigation, command and control, and weapons' targeting and operation. Cyber weapons also can have much greater impact on infrastructure and physical systems than traditional instruments of electronic warfare can. Major powers have already used such offensive cyber capabilities against others, but they have not directly engaged each other

in escalatory warfare in the cyber era. Thus, there is no empirical basis or analogy for evaluating how the dynamic competition between enabling and disabling cyber operations would play out in actual combat among near peers.

Operational Challenges

The enabling and disabling functions of cyber capabilities can serve both offensive and defensive purposes. While this is true of other intelligence-gathering tools and weapons too, the duality of cyber capabilities and their technical and operational features render them especially ambiguous. States often claim (fairly or not) that their military actions are defensive and precautionary while their opponent's activities are aggressive. This should be expected in the case of cyber operations also. The ambiguous offensive-defensive duality of cyber tools, operations, and, in some cases, organizations (like computer emergency response teams) raises challenges similar to those posed by national ballistic missile defenses in nuclear-armed states. Building effective defenses on a scale that could match an opponent's nuclear-armed missile arsenal could be a way to lower the risk of initiating offensive attacks (by blunting the victim's capacity to retaliate); yet, declarations of purely defensive intent in peacetime do not obviate the physical capacity of such capabilities to augment offensives in wartime.

The ambiguities that inhere in cyber operations are not simple to resolve. Means and procedures for clarifying intent have yet to be developed. Here the difficulty is that clarification of intent hinges at least in part on the willingness of actors to disclose the penetrations they have achieved or for the defender to reveal to a prospective attacker that its penetration has been detected. Both steps would be fraught with acute dilemmas.

In terms of target disablement and destruction, three types of weapons discussed in this volume merit comparison with potential cyber weapons. Robert Schmidle, Michael Sulmeyer, and Ben Buchanan in chapter 2 describe how experience with nonlethal weapons such as pepper spray, temporarily blinding lasers, foam guns, and road spikes to puncture vehicle tires may suggest potential applications of cyber weapons. Nonlethal weapons are meant to incapacitate rather than destroy an adversary's equipment and personnel. This incapacitation would often be localized, temporary, and possibly reversible. These effects could make such weapons relatively benign and therefore politically acceptable to use. Cyber weapons can achieve such effects via denial of service attacks or corruption of a military system's operation, as Israel reportedly did with Syrian air defenses in the 2007. Cyber attacks on cellular phone and other communications systems can disrupt the capacity of actors to coordinate illegal, hostile, or otherwise dangerous behavior without physically harming these actors and innocent people nearby. But, equally, such attacks may complicate efforts to terminate a conflict because communications between the political leadership and the field may be undermined.

On the one hand, nonlethal weapons have been and are most likely to be used in overt conflicts short of warfare. The distance from which cyber weapons can

be operated, and the difficulty of attributing their use, makes them even more appealing for gray-zone operations than are other lethal and nonlethal weapons.

On the other hand, the challenge of confidently predicting and limiting the effects of cyber weapons may make them more difficult to apply than other nonlethal weapons are. As Schmidle, Sulmeyer, and Buchanan note, "With capabilities as new and complex as cyber ones, the unintended consequences of particular capabilities may cause additional or unexpected damage." The uncertainty—which includes possible over-performance or under-performance—then "greatly complicates the confidence a commander can have in the ability to achieve precise effects exactly when desired." This uncertainty may lead to self-restraint in opting to use them, as has been the case with nonlethal weapons. Yet, in overt warfare, when destruction and civilian casualties are already occurring, this inhibition presumably would decrease.

For purposes of destruction, as distinct from temporary disablement, PGMs such as guided gravity bombs and cruise missiles have been especially attractive to those states that can acquire them and support their use with adequate targeting information. The comparative advantage of these weapons lies in the precision, the exchange ratio, and the probability of destruction, especially as their operational ranges grow. Cyber weapons can have similar advantages. Unlike PGMs, cyber weapons do not require expensive, observable platforms and extensive logistical development and support infrastructure. But, as James M. Acton explores in chapter 3, cyber weapons may pose more challenges for their users than PGMs do.

First, in any missile or cyber attack, precision depends on the accuracy of the targeting coordinates and the effects of the weapon. A missile aimed at the wrong target or a malware attack on a network whose connections were not accurately mapped by the attacker can result in adverse consequences for the attacker (as well as the victim). The potential scale of unintended (imprecise) effects of cyber attacks, however, could be significantly greater than that of a cruise missile or bomb because of the lower certainty about the desirable and undesirable effects of their employment. For example, the cyber weapon could fail to neutralize the target, or malware used in an attack could spiral out of control or could be reverse engineered and proliferated by adversaries. The latter is an especially grave concern for cyber weapons, analogous perhaps only to biological weapons.

Second, the intelligence collection required for accurate, effective targeting of weapons is in some circumstances greater for cyber attacks insofar as the attacker needs to learn not only how to enter a network but also its extent, how it works, and what consequences any attempts to manipulate it might have. Moreover, targeted information and communications systems are not "stationary" as some prime targets of PGMs would be. Software is regularly updated, hardware is replaced, security protocols are changed, vulnerabilities are discovered, and so on. In the future, as offensive and defensive cyber systems become more automated, adoptive, and artificially intelligent, the challenge of attacking

them will be akin to targeting mobile missiles, which is quite daunting though not impossible.

Third, as with PGMs, attackers need to be able to assess the damage they inflict on targets in a timely manner. Aviators conducting a bombing raid on a suspected nuclear plant need to know that the targeted country's air defenses have been disabled, whether by missiles or malware, before the planes come into range. As Acton suggests, the need for quick and reliable battle damage assessment may be even greater for cyber attacks in time-sensitive military operations insofar as their effects can be temporary, reversible, and less observable. A cyber attacker seeking to disable a set of adversary capabilities in order to conduct other operations needs to know not only that the degradation of their performance has indeed occurred but also when they may be fixed. Making such damage assessments is also vital to figuring if and when malware has spread unintentionally to other targets that might cause political, diplomatic, economic, or strategic harm to the attacker's position. Knowing the full extent of damage that has been or may be caused is necessary to inform efforts to neutralize or minimize unintended effects and to manage the consequences, including with parties not involved in the conflict.

Fourth, while cyber weapons might be used repeatedly over a short period, they are not likely to be usable in multiple successive campaigns against the same adversaries, unlike aircraft and missiles. Further, once adversaries (and the global information technology community) detect malware, they can develop ways to defend against it in days or months rather than the years or even decades required to develop new defenses to advanced kinetic weapons.

Finally, and importantly, PGMs with few exceptions do not achieve strategic objectives. Similarly, cyber capabilities may deter and coerce states and nonstate actors or, theoretically, serve as firebreaks against escalation in crises or war, but they don't win wars, remove governments, end insurgencies, or restore order to regions beset by violence. As Acton writes, "Even if cyber attacks prove highly effective at disrupting an enemy's [buildup and] military operations, physical force will almost certainly be required to exploit this disruption." This is not to deny that governments, depending on the circumstances, can use cyber capabilities to undermine or influence the composition of other governments and to intimidate and weaken internal opponents. Opponents of governments can use cyber capabilities to do the reverse too. The larger point here is that, to take and hold power, actors likely will need other capabilities to consolidate opportunities created by cyber operations. For example, as Peter Feaver and Kenneth Geers note in chapter 13, every facet of the conflict in Ukraine has been affected by cyber attacks, yet "the cyber dimension of the conflict has nonetheless not played a critical role in the war."

Weaponized drones are an advanced form of PGM. They are especially attractive for targeting single or small numbers of people or other soft targets over long distances with an extremely short time between the decision to fire and the impact on the target. To date, drones have not been used to attack substantial

matériel, infrastructure, or military targets, although their payload and lethality are rapidly increasing.

As David E. Sanger records in chapter 4, drones and cyber weapons share a number of advantages, notwithstanding the different types of targets they are directed against. They are relatively cheap to procure and operate. They do not put their operators at risk. For intelligence-collection purposes and for attack, drones can hover over targets for long times, helping reduce risks of mistaken targeting and unintended casualties. Cyber assets can reconnoiter targets for even longer periods.

While the destructiveness of missiles delivered from drones can be predicted precisely, and drone reconnaissance reduces risks of targeting errors compared with aircraft or cruise missiles, their primary liability remains mistaken targeting. A wedding party is killed because it was misidentified. A family believed to include the leader of the Islamic State is killed in a strike on a house that would have been acceptable to the leadership of the attacking state and perhaps under international law and public opinion, but due to faulty (or dated) intelligence, the leadership was not there. Cyber weapons are not equally prone to the consequences of mistaken identity, because thus far they are not (and perhaps in the future they will not be) used primarily to injure or kill people as opposed to disabling the systems the people depend on for various purposes. Nevertheless, as Sanger reports, uncertainty over effects and the related risks of collateral damage have inhibited the broad-scale use of offensive cyber weapons by the United States and probably by other countries too.

Risk of proliferation is another inhibitor of cyber attack that pertains less to drones. The software and operational techniques used to mount a cyber attack could be captured and replicated by adversaries, perhaps with attribution to the attackers. This risk of reverse engineering obtains with drones too, of course, but copying drone technology takes longer than copying and adapting malware. Further, drones are not nearly as versatile and potentially dangerous as cyber weapons are. Nor can most adversaries as easily deploy drones over long distances as they can cyber weapons.

On the other end of the war-fighting spectrum from drones, cyber weapons, in theory, can achieve large-scale effects on war-supporting facilities and infrastructure that otherwise might require extensive bombing campaigns to destroy. Norms and laws of armed conflict have evolved since World War II so that widespread indiscriminate bombing by states is now taboo. (This proposition has been tested by the destruction visited on Syria, including by Russian attacks; by the Sri Lankan government's prosecution of civil war against the Liberation Tigers of Tamil Eelam; and by the attacks of hybrid organizations such as Hezbollah, Hamas, and the Islamic State.) In any case, states engaged in overt warfare today increasingly seek to target their adversaries' war-supporting infrastructure, especially energy production and transmission resources, as well as telecommunications networks and services. The scale and intensity of operations required to achieve these results with surgical application of kinetic weapons

could be daunting both for the potential target states and their populations and for the states that would conduct such attacks due to the risk of dramatic overkill. To the extent that cyber weapons could surgically undermine the functionality of war-supporting facilities, infrastructure, and industry with much less destruction of life and property, and lesser permanent or environmental damage, such weapons may be relatively desirable. Indeed, the option of first trying to hit a target with a cyber weapon and, only if and when that fails, then resorting to kinetic attack is appealing.

Yet three caveats must be raised. First, as noted earlier, there are significant uncertainties regarding the effects of malware attacks over time. The development of the field of operations research for offensive cyber operations is merely in its infancy. Second, if superiority can be attained in the ability both to inflict damage and to confidently limit effects, the inclination to conduct such attacks may grow. Third, if an adequate level of defensive protection exists to limit the prospects of retaliation, then incentives to conduct attacks will increase. Each of these three possibilities can be destabilizing; however, they also can be stabilizing if the credibility of threats to conduct precision cyber attacks strengthens deterrence of wrongful actions. Hence, the impact of introducing offensive cyber capabilities is highly context specific, as we discuss further later.

On the ultimate end of the spectrum of destruction lies attacks on major population centers via weapons of mass destruction. International humanitarian law and the laws of armed conflict proscribe such attacks per se. Nuclear-armed states nonetheless plan to target leadership, military command and control, and other strategic assets that are located amid or close to population centers. Moreover, those actors willing to violate international norms and laws could use nuclear and perhaps biological weapons for massive destruction.

Cyber weapons raise several questions in this context. First, is massive disruption meaningfully distinguishable from massive destruction? Steven Miller in chapter 10 notes that "any use of nuclear weapons will have devastating consequences. The same is not true of cyber." While this assertion is undoubtedly true in a political sense, it is less certain in physical terms. A single high-altitude nuclear detonation, say, in a desert or over a ship at sea clearly would not cause widespread destruction. But while a nuclear warning shot could cause an opponent to eschew further escalation of conflict, in the case of a nuclear dyad it also could have the opposite effect and unleash an escalatory exchange of nuclear weapons, leading to mass destruction. There is no data on limited nuclear warfare, only conjecture. If cyber weapons could be unleashed to massively disrupt or disable—even temporarily and reversibly—systems on which whole societies depend without directly killing large numbers of people, would such use be more likely and, if so, with what justification? How would the potential availability of achieving mass disruption by cyber operations affect the behavior of states in crises or in escalating warfare? In potential conflict among nuclear-armed states, could the use of cyber weapons to inflict massive disruption of the adversary's military and economy be a less objectionable alternative to nuclear attack? Could

this cyber option, especially when intended as a political signal, act as a firebreak to nuclear escalation and thereby reduce the risks of nuclear war?

Again, nuclear war has not been experienced between adversaries who both possessed these weapons. Many argue that the unique, horrifying, and irreversible destructiveness inherent in nuclear weapons has encouraged restraint and, to date, made mutual deterrence work. In contrast, cyber attacks have become commonplace, albeit on a limited scale thus far, and clearly have not exhibited the mass-disruption potential they are widely believed to possess. Does the relative nondestructiveness of cyber weapons open the way to their potential use to achieve massive disruption? Or is the inability to confine and predict their effects (much as with biological weapons) a major cause of restraint? And would this unpredictability make deterrence as developed in the nuclear domain less tenable, as Steven Miller suggests?

Cyber weapons are more analogous to biological than to nuclear weapons in terms of their low visibility and the type of effects they could have.[1] Thankfully, experience with biological weapons is limited, and the possession and use of these weapons are now banned by the Geneva Protocol of 1925 and the Biological Weapons Convention of 1972. The latter has not been universally signed or adhered to, and it does not preclude some future use of biological weapons that could have implications similar to cyber warfare. But for now it can be said the restraints on biological warfare are far greater than those on cyber warfare. On the one hand, as with biological weapons, the development, penetrations, and attacks—for offensive and defensive purposes—of cyber weapons could go undetected, at least for a time. They could remain concealed even after indications of their existence appeared. At least for some time, it could be difficult to distinguish reliably whether an effect was due to an attack or a natural occurrence, further complicating attribution in case of attack. Biological attacks, like cyber attacks, can have minor effects and can be temporary and eradicable. On the other hand, some cyber and biological attacks could be immediately detected and identified as such, and they could cause extensive and long-lasting damage. Just as with biological weapons, their effects may hinge on numerous factors, some of which are transient, thereby creating serious uncertainty about their real-world effects and further undermining the capacity to precisely tailor the damage they inflict.

The Contingent Future of Cyber Weapons

To summarize, the versatility of cyber weapons, the unbounded distance over which cyber intelligence gathering and attack can be conducted, the safety that cyber technologies afford their operators, the secrecy and difficulty of attribution they entail, the low cost of attacks, and the potential precision and reduced violence of their effects—all make these weapons not only more tempting to use but actually more usable than other coercive instruments are. Is their overall impact, then, stabilizing or destabilizing? If the uncertainty over attribution and the reduced scope, level, and duration of damage imposed by cyber weapons

make states (and others) less inhibited to conduct such attacks, war and its escalation could become more likely. In parallel, the attractiveness of versatile cyber capabilities could diminish states' attention to and investment in diplomacy and other instruments of statecraft. Conversely, cyber weapons could be unusually stabilizing in two ways—if the relative utility of cyber weapons makes them a credible instrument of deterrence or compellence and if they can serve as an effective firebreak against further escalation, thus reducing incidents of conflict or capping escalation in crises. The flip side is that many, if not most, of the states that are most capable of deploying potent cyber weapons are themselves vulnerable to the damage such weapons can inflict. Moreover, the uncertainty of cyber weapons' effects and the risk that malware can be replicated and proliferated relatively easily have made leading cyber states cautious in using them, at least to date.

Overall, it is important to recognize that this new technology is not deterministic. Great uncertainty and contingency exist in this domain. Manifold potential scenarios for war fighting, deterrence, and restraint can be imagined. They are central to the future that states and societies must struggle to shape, as we discuss in the next two sections.

What Might Cyber Conflict Be Like (or Not)?

Having drawn on analogies to summarize some of the distinguishing qualities and effects of cyber weapons, and some of the advantages and challenges these qualities and effects pose, we now consider what conflicts involving these weapons might be like.

Information Warfare

Stephen Blank describes in chapter 5 how Russia has incorporated cyber technologies and operations into its long-standing approach to political warfare and information operations to unnerve, weaken, and otherwise intimidate adversaries. In Georgia and in Ukraine, actors believed to be motivated by Russia placed malware in electricity supply systems to deter Russia's adversaries and others from escalating competition. In the case of Ukraine, a malware attack was unleashed, apparently in retaliation for a physical bombing of transmission lines feeding Russia-controlled Crimea and to signal the capacity to inflict greater damage on Ukraine. Following the imposition of Western sanctions on Russia, Russian cyber actors massively penetrated major US banks but were not reported to have stolen money or corrupted data. This suggests that the purpose was to deter the United States from pushing for more sanctions against Russia. Russia apparently interfered in the 2016 US presidential election, presumably to dissuade the United States from sanctioning or otherwise contesting the Russian government's behavior at home and in the "near abroad." The general point is that cyber capabilities can be potent tools for waging political warfare and deterring adversaries from countering such exertions in escalatory ways.

Preventive and Preemptive Use of Force

Preventive war and preventive use of force have been undertaken throughout history; likewise, cyber capabilities may be applied for both purposes. As John Arquilla describes in chapter 6, preventive war generally involves "starting a war at a most opportune moment . . . while the prospects of defeating an enemy's military, seizing territory, or toppling a regime are good—or at least before a growing threat worsens." Preventive force, by distinction, seeks to apply measured violence "in the hope of avoiding a full-blown war or to keep the strategic situation in an ongoing confrontation from deteriorating." (Preemption is different still, referring to action to defeat or weaken an adversary's *imminent* attack).

For various reasons, as Arquilla suggests, preventive force has become a common feature of international affairs in recent years and is likely to take cyber forms in the future. The Stuxnet attack is the leading example of using cyber force to prevent nuclear proliferation, to reassure allies, and thereby to avoid conventional war with Iran over its nuclear program. Other purposes could be to deter adversaries from aggression or to compel them to change their behavior and thus avoid suffering a wider-scale cyber or kinetic attack. Cyber attacks can be used against adversaries' offensive cyber capabilities and to degrade conventional military or other assets that are enabled by cyber systems and therefore are vulnerable to cyber attack.

Arquilla recounts how Britain's preventive uses of naval forces against Denmark (and indirectly France) in 1801 and 1807 succeeded in their immediate objectives of thwarting Napoleon's naval ambitions. But these successes also had the unintended effect of spurring Germany's subsequent century-long buildup of its naval forces and other defenses against British naval mastery. Analogizing to cyber preventive warfare, Arquilla posits that cyber techniques offer greater potential than kinetic weapons for protracted efforts to retard or delay an adversary's acquisition of dangerous capabilities and its conduct of aggression. In particular, "cyber prevention might also prove an ideal means for detecting and disrupting terrorist networks, for slowing their recruitment processes, and for generally undermining [their] trust and morale." The advantages of cyber stem in part from the covertness and difficulty of detecting and diagnosing correctly cyber capabilities and operations. These issues may provide both operational and political advantages to the attackers, especially the more tech savvy among them. If an attacker can initially mask the failures that are induced as a mere technical accident and subsequently plausibly deny involvement and keep personnel out of harm's way, the risks of being held publicly accountable and sparking escalatory retaliation appear much less than would be the case if other means of attack were used. However, once used, a particular cyber weapon can be detected, countered, and adapted by adversaries for their own use. For these and other reasons, the preventive use of cyber weapons can cause and intensify arms racing. Ultimately, Arquilla concludes, cyber preventive force is likely to increase, and it is impossible now to predict whether on balance the consequences will be welcome or unwelcome.

Preemptive use of force differs somewhat from its preventive use and is likely to be an attractive role for cyber weapons. Preemption occurs when conflict appears imminent or unavoidable, and preemptive attack appears to offer some prospect of significantly diminishing the adversary's capacity and will to prevail. States and non-state actors increasingly envision how they could use cyber attacks to preemptively weaken adversaries' conventional and cyber potency. At the same time, states and societies that depend heavily on ICTs feel acutely vulnerable to preemptive surprise attack. One actor's vulnerability is another actor's opportunity.

The Japanese attack on Pearl Harbor in December 1941 is, at least for Americans, emblematic of such a preemptive attack. Chapter 9 by Emily O. Goldman and Michael Warner usefully dispels the common misunderstanding that Pearl Harbor was a "bolt from the blue." Relations between the United States and Japan already were conflictual. The United States was crippling Japan's economy with sanctions to compel it to quit China. Washington expected war. In this sense, the Pearl Harbor attack was a preemptive escalation of an existing conflict. If anything, what happened at Pearl Harbor is now more germane to current situations in Europe, the South and East China Seas, the Korean Peninsula, and the Middle East, where competitors are engaged in disputes and mobilizing coercive capabilities and policies to influence each other. The Pearl Harbor analogy invites analysis of how cyber attack could be integrated into, or even stimulate, preemptive combined-arms warfare.

The purpose of the Pearl Harbor attack was to weaken and delay the capacity of the United States to prosecute a war with Japan, which hoped that it would diminish the resolve of Washington and the American people to fight and instead would motivate accommodation with Japan. In the cyber era, an analogous purpose of a preemptive attack could be to disable and disrupt a stronger power's capacity to deploy distant forces while creating time and space to achieve initial victories against extant forces. If a cyber attack could be counted on to reliably inflict relatively minimal casualties or damage to an adversary's forces, unlike the kinetic attack at Pearl Harbor, then such an attack could alter the strategic context of a confrontation by presenting the adversary with a fait accompli at minimal cost to both parties. The burden of escalation would shift to the state seeking ingress on the other's territory, advantaging the side that conducted the preemptive cyber attack. (Of course, an ingressing state also could attempt a preemptive cyber attack to weaken the receiving side's capacity to repel it, with the goal of motivating the defender to accede to the attacker's demands.)

In the case of Pearl Harbor, the attack failed both tactically and strategically in ways that may offer lessons for potential cyber preemption. The Japanese attackers missed the US Pacific Fleet's more important aircraft carriers, heavy cruisers, and submarines. The attack also did not destroy or durably incapacitate the fleet's fuel depots, dry docks, repair facilities, and undersea cable landings. By analogy, an actor contemplating a preemptive cyber attack against a powerful adversary would (should) need confidence both that intelligence on the systems being attacked is comprehensive, accurate, and timely and that the predicted physical

and strategic effects of the attack are accurate. Significant overestimates of effects could mean that the adversary would be insufficiently damaged, while significant underestimates of effects could mean the adversary (and other states) would become more, rather than less, motivated to escalate in response. Relatedly, to calibrate the next steps, the cyber attacker would need accurate and comprehensive assessments of the damage caused by the attack. The attacker especially would wish to know how much time would be available before the adversary could remobilize capabilities that had been disrupted. Japanese leaders made both mistakes in the Pearl Harbor attack, underestimating the extent of the damage it would inflict and the motivation it would give the United States to fight.

Pearl Harbor also provides lessons for defenders against cyber attack. Had the Japanese attack significantly destroyed the Pacific Fleet's logistics capabilities, the attack would have achieved more lasting effects. Among other things, this highlights the importance of defending a state's logistics capabilities, and the infrastructure required to sustain it, from cyber attack. In the cyber era, military logistics are extremely dependent on ICT and the backbone of the Internet, with all the vulnerabilities this reliance entails. In many states, the entities and systems involved in logistics are controlled by private sector contractors and not exclusively by governments. Thus, the challenge of defending them is enormous, complicated, and very costly. Huge numbers of personnel and organizations, operating under diverse cultures and institutional imperatives (including cost management), must be trained repeatedly and harmonized to keep defenses effective and current. Resilience—again complicated and costly—must be built into the networks required to supply and operate military forces.

No one now has the experience of conducting or defending against a major cyber attack analogous to Pearl Harbor. Potential attackers and defenders, therefore, do not really know whether and how their capabilities to conduct and defend against a major preemptive attack would operate in real-life interactive conditions. The reconnaissance of adversaries' networks and the deployment of tools required to prepare an attack could be negated through routine actions taken by defenders to surveil, maintain, and upgrade their systems. Optimistically, states could deploy early warning sensors internationally, including in adversaries' systems, and marry them to active defenses to blunt attacks. Such defenses could be automated either as a default condition or in response to a command during crisis. All these possibilities create a premium on early action—simultaneously offensive and defensive—in a potential war situation to exploit vulnerabilities in the adversary's systems before any hostility begins ("use it or lose it") and to thwart an attack before one suffers losses. These incentives, amid the broader uncertainties of how interactive cyber war would actually unfold, highlight the potential of misunderstandings and miscalculations triggering preemptive attack and escalation, all of which can be destabilizing.

Escalatory Warfare

World War I provides a different example of war being triggered by an act whose timing and nature were unpredicted and then escalating with a scale and pace

that leaders were unprepared to manage. Some fear this could be a likely course for a cyber conflict. No one foresaw that a Serbian terrorist cell, with ambiguous ties to the Serb state, would attack the heir to the Habsburg throne and thereby instigate a war involving all the world's major powers and killing seventeen million people. The governments and societies that then moved step by step into massive warfare did not imagine how it would escalate and persist. Early historical accounts of the war argued that technology—specifically, rail transport—drove the escalation process.

The question pertinent to analogizing World War I and potential cyber conflict is whether technology—railways in World War I and cyber today—importantly affects crisis stability and whether a conflict once started will escalate. The Balkans were a tense region at the beginning of the twentieth century, with lingering territorial and political disputes and competitive major powers jockeying for advantage directly and via proxies. This description also pertains to the Middle East, Russia's periphery, and South and East Asia today. Similarly, it is possible, especially in the Middle East, the Russian periphery, and the Indian subcontinent, that actors with relationships that are difficult to attribute conclusively to states could commit acts that other states would perceive as aggression.

In 1914 once a terrorist attack occurred and precipitated the crisis, Germany, France, and Russia had powerful incentives to mobilize their troops and railways first, before their adversaries did. Railways compressed space and time—key variables in military conflicts—and thereby increased pressures on decision makers during a crisis. This compression coupled with the technical challenges of reversing course (rerouting traffic) rigidified response options, resulting in a strong first-mover advantage. The space and time for managing the crisis narrowed. Thus, following the June 28 attack on Archduke Franz Ferdinand, the competing powers felt imperatives to move quickly to mobilize their forces. Once mobilization began, it created momentum toward conflict that was difficult to arrest or reverse, especially as little time was allowed for deliberations and diplomacy. Yet, even if leaders had wanted before the war to negotiate measures to regulate or limit military uses of railways, this effort would have been severely complicated by the imperative not to undermine the great economic benefits of this technology.

Francis J. Gavin, in chapter 7, carefully sketches this dynamic while taking pains to emphasize that railways did not cause World War I. Political factors did. The idea that new military capabilities, especially railways, would advantage the offensive and make war short and decisive "created a more permissive environment for states to gamble and risk war." But this did not determine events. Moreover, railways themselves were potent only insofar as they were integrated with military forces that could take and occupy territory. Similarly, cyber capabilities *alone*—even if, unlike railways, they can directly cause extensive damage—cannot by themselves fight and win large-scale wars and determine postwar outcomes. Achieving these strategic purposes requires a mix of cyber and other major military capabilities, but cyber operations could certainly compress the

time and space for diplomacy and create serious incentives to undertake preemptive action in a crisis situation.

The conflict-hastening potential of cyber weapons could be partially mitigated by robust defenses against cyber attack and by resilient communications and command-and-control systems. Such robust passive defensive measures were not available to counter railway mobilizations. But it remains uncertain whether and how states would have confidence in their defenses and resiliency given the nature and rapid evolution of offensive cyber capabilities. This observation points to the importance of political institutions within states and diplomatic processes among them. Europe in 1914 was woefully underinstitutionalized. The capacity to mobilize massive numbers of soldiers and military equipment grew much faster than each state's ability to accurately assess, share, and deliberate on such mobilization and then collectively to negotiate measures to control escalation. More developed institutional capacity would not have prevented the terrorist act in Sarajevo, but it could have averted or contained the escalation that followed it. This observation is pertinent for Indo-Pakistani relations today as well as for regional tensions in the Middle East and perhaps East Asia.

Economic Warfare

The World War I era invites cyber analogies in part because the economy of that time was more globalized than ever before and after until the information and transportation revolution took hold in the 1990s. In the early 1900s, as Nicholas A. Lambert narrates in chapter 8, "accurate and instantaneous information relaying details of supply, demand, and prices was essential to all businesses and especially to the financial services industry that facilitated the movement of commerce with ever-increasing velocity." Connectivity created the potential to attack vital nodes of a country's economy or the global economy, as it does today. British naval strategists in the ten years leading up to August 1914 sought to leverage the combined supremacy of London's available commercial maritime information and the Royal Navy's command of the seas to develop plans to wage strategic economic warfare. Their aim was to quickly shock and derange the enemy's entire economy, thereby driving German society to abandon support for its misguided government. This differed from the "strategic" bombing campaign later practiced (and mislabeled) in World War II that targeted military and related industrial assets such as ball-bearing plants, aircraft manufacturers, and oil refineries. The broad analogy today to what the British had planned in 1914, obviously, is to a massive cyber attack on national and international financial institutions or other critical infrastructure that would promptly cause chaos, economic paralysis, enormous financial losses, and so on.

Britain's hegemonic position at sea and in global trade and finance enabled its officials to imagine this strategy. Their optimism was bolstered by the British economy's capacity to withstand the financial and economic shocks that a war would bring better than all other major powers could. These observations prompt

analogous questions for the cyber world. Is hegemony different in cyberspace than, say, on the ground, at sea, and in the air, where armies, navies, and air forces heretofore have determined hegemonic power? Does any single power, most likely the United States, have sufficiently more capacity than any other power to combine financial intelligence and cyber superiority with physical power projection to gain a decisive capacity to influence international affairs and win conflicts? And does the power of a particular state to exert its will in cyberspace come with a corresponding vulnerability to cyber exertions of other actors against it? It took a long time for competitors to build navies to contest the British and for alternatives to British traders and financiers to rise. In cyberspace, are capacities and vulnerabilities more readily changeable?

The potential "disruptiveness" of the British economic warfare strategy inspired years of secret debate within the Admiralty and between it and other departments of the government, including the Board of Trade, the Treasury, and the Foreign Office. Officials perceived that the strategy could not only be effective but also have unprecedented and perhaps unforeseeable implications for Great Britain and for national and international law. The British process leading up to the strategy in 1914 resembles more recent accounts of US governmental deliberations over various forms of offensive cyber operations whose implications would be uncertain and unprecedented.

When hostilities in Europe started, purposeful economic strangulation compounded the natural contractions of war, as planned. But the ensuing unintended tightening of finance, trade, production, and employment was so alarming that British workers, businesses, and political representatives turned on the government. So did neutral countries that were damaged collaterally. Within three months, the British government aborted the economic warfare strategy. In a sense, it had been too effective. Its consequences were so sharp and widespread that they hurt British interests too, and political leaders could not ignore them.

Would a cyber campaign to inflict massive disruption on another state's economy yield similar blowback that could render it unsustainable and therefore strategically of little value? Would this be true for any state or only for some? Can cyber attacks be designed and conducted to achieve *massively* disruptive economic effects on a targeted state or group therein without harming others and the global economic and financial system as a whole? Would the risks of blowback depend significantly on the level of dependence on international connectivity of particular states and societies? For example, would Russia be significantly less susceptible than the United States or the United Kingdom or even China would be to blowback if Russia conducted cyber attacks against its adversaries' banks that in turn led to a crisis and major losses in the global financial system?

Strategic Context

The analogies presented in this book to explore what cyber conflict might be like are far from exhaustive. Two broad contextual possibilities for future cyber conflict deserve brief additional discussion here. The first centers on conflicts

between states that clearly are unequal in aggregate capability to conduct nuclear or conventional warfare, covert operations, and cyber warfare, as distinct from conflict among near equals. The second centers on potential conflicts between nuclear-armed states.

Exemplifying the first context, the United States and Israel have used drones to attack adversaries in Afghanistan, Yemen, and Gaza that lack defenses against this technology and commensurate counteroffensive capabilities. The United States has used PGMs similarly against adversaries that cannot defend against them or retaliate long distance to threaten the US homeland. In circumstances where opponents were more evenly matched, the probability and conduct of offensive operations presumably would be different. A central question, then, is whether the accessibility of cyber war-fighting capabilities, and the global reach they provide, would significantly change the correlation of forces between adversaries that otherwise are highly unequal in coercive power. That is, do cyber capabilities offer the potential to further consolidate the stronger power's absolute advantage, or, conversely, do they enable weaker actors to shift the balance of power?

We are obviously unable to provide a definitive answer here, yet the Israeli experience may be illuminating. Notwithstanding Israel's overwhelming superiority in both unmanned aerial vehicle and cyber technologies, as well as other military capabilities, Hezbollah and at times Hamas have been able to achieve a conventional balance of terror by acquiring inferior but nonetheless meaningful retaliatory capabilities. This balance, though precarious at times, has largely confined the confrontation between the adversaries to sporadic, mostly short-duration exchanges that have denied the stronger party conclusive achievement of its aims. Offensive cyber capabilities could have similar strategic effects in confrontations among "unequals."

Finally, most of the states with active offensive cyber capabilities also possess nuclear weapons, with Iran being a notable exception. Thus, in competitions and warfare between these states and between them and other adversaries, the shadow of nuclear deterrence will be visible. Conflict, including with cyber dimensions, that could begin or threaten to escalate to major warfare will carry the potential to go nuclear. Nuclear-armed states, to date, have not conducted such warfare against each other (or allies of nuclear-armed states). Many observers attribute this to nuclear deterrence. Thus, possibly, and perhaps likely, deterrence of *major* warfare among nuclear-armed states will persist regardless of whether cyber attacks are unleashed.

Two caveats to this observation must be offered. First, cyber attacks on strategic command-and-control systems could be attempted to negate an adversary's nuclear deterrent. This possibility is especially worrisome in situations where the first use of nuclear weapons in escalating conventional war, even their tactical use, is real—for example, in Pakistan or perhaps North Korea. The threat of cyber attacks on strategic command-and-control assets could then cause that adversary to take countervailing steps, including using (or at least pre-delegating the use of) nuclear weapons earlier than otherwise expected, to

avoid or minimize losses to its nuclear forces. This challenge is greatly aggravated by the similarity between cyber penetration of the nuclear command-and-control systems for purposes of intelligence gathering and early warning on the one hand and offensive operations against these systems' functionality on the other hand. Second, if cyber attacks were perceived to be attractive because a state believed they would fall below the adversary's threshold for nuclear escalation, and such attacks then had unexpected massive effects, nuclear escalation could inadvertently result. In any case, the relevance of nuclear deterrence is important in the cyber era, and it should be remembered that none of the analogies in this volume involve warfare among nuclear-armed states.

What Is Managing Cyber Conflict Like (Not Like)?

The cyber attacks on Estonia and Georgia in 2007, Iran beginning in 2007, Sony Pictures Entertainment in 2014, and the Ukrainian electricity system in 2015, as well as the hack into the US Democratic National Committee in 2016, reflect how criminal activity and interstate confrontation are now channeled to and through the cyber domain. In terms of its centrality on the international agenda, cyber confrontation is assuming the role that nuclear weapons occupied during the height of the Cold War. We invoke the term "confrontation" as a background condition to convey that the actors that may find themselves moving toward conflict cannot easily be categorized as aggressors or defenders. Some states and non-state actors, for example, dispute sovereignty over territory, with each claiming to be right. Some dispute the legitimacy of governments and feel the need to compel them to end repressive behavior; others feel the need to prevent or punish interference in their domestic affairs. The classic dichotomy of offense versus defense, however, does not capture the nature of confrontation in cyberspace. This is not merely because some of the purposes of cyberspace activities are either indistinguishable or mutually reinforcing. Many major contestants are acting, or preparing to act, offensively and defensively at the same time while using the same basic instruments for both efforts. The action is persistent.

Notwithstanding the persistence of confrontational interactions, most of the actors on the world scene need the cyber domain to function stably enough so they can operate in it both nationally and internationally. Thus, there is a tension between one's potential interest in using cyber operations to exercise control over one's population or to weaken or otherwise harm adversaries, and one's interest in preserving the functionality of the global cyber system. Each competitor wants to exert itself as fully as it can against its adversaries, but each objectively has an interest (though not necessarily of equal salience) in not causing a total breakdown in the functioning of the system itself.

The stability of the cyber system and of the broader political economy are now more connected than ever. In both cases stability is dynamic, not static. Both feature constant change, disruption, and creation. Systemically destabilizing actions would be those that exceed the normal flux of change and competition and that destroy or severely undermine the functioning of cyber communications and

commerce and/or the broader political economy. Cyber conflict has the potential to threaten both systems. Acts that deeply and durably sow doubt in the reliability and integrity of the international cyber system—or otherwise disrupt its functioning, much less destroy it—would also cause international economic crisis. Major interstate warfare with cyber aspects would likely threaten both the cyber system and the broader geopolitical system.

Objectives in Preventing and Managing Cyber Conflict

To prevent or minimize activities that threaten the functioning of the global ICT system and the global political economy, states and relevant private actors should be expected to undertake a range of policies and activities to fulfill the following functions:

- enhance the capacity to detect and attribute cyber exploitations and attacks and to distinguish their purposes;
- augment various forms of defense against such activities, both to protect assets and raise the costs to potential perpetrators;
- increase the resilience of key cyber-dependent systems;
- while more difficult, pursue political and technical analogues to arms control agreements, or understandings that could inspire confidence that malware and other "weapons" will be sparingly used and will not have unintended consequences, including proliferation;
- assert state control over actors that use their territories to conduct unlawful cyber activities and over their citizens who do so abroad;
- upgrade capabilities to signal, threaten, and initiate cyber and other actions to inflict sufficient "pain" on adversaries to motivate them to eschew or desist from hostile activities; and
- develop, over time, norms to restrain the most potentially destabilizing sorts of cyber activities.

These steps would contribute to the prevention and mitigation of actions that could threaten the dynamic stability of the cyber domain and of the international political economy.

Defensive Measures

States and private actors are increasingly devoting resources to detect cyber intrusions and possible attacks. Little tension or debate affects such salutary efforts. Yet other steps or forms of defense do elicit various concerns relating to cost, legal propriety, and international stability.

Defensive capabilities and operations are, and will continue to be, central to preventing and contending with cyber attack in ways that are very different from countering nuclear attack, for example. "In stark contrast to a nuclear attack," Peter Feaver and Kenneth Geers write in chapter 13, "most cyber attacks can be stopped—at least in the tactical sense—with purely defensive measures." Moreover, many ways exist, and can be developed, to defend against cyber attacks

without resorting to counterattacks that inflict damage outside of those networks being defended. Security "hygiene" within networks and organizations, anti-malware tools, and honeypots to lure or deflect attackers into isolated systems are well known. Other techniques could include analogues to emplacing "dies" in data the way banks do in cash so that if data or software are stolen, they become marked or do not "work" when located in unauthorized systems. Beacons can be embedded in data to emit signals if and when they are stolen, augmenting the capacity of authorities to trace perpetrators. Such defensive measures can raise the risks and potential costs of illicit cyber activity without eliciting dangers of unwanted or difficult-to-manage conflict.

However, as John Arquilla's "harbor lights" analogy warns, even the most seemingly obvious and risk-free defensive measures—turning the lights off to avoid being targeted at night—may not be taken due to organizational dysfunction, fear of protests by those who might be inconvenienced, market pressures on technology producers to minimize costs and operational complexity for users, and concerns of intelligence and law enforcement interests who want to maintain opportunities to penetrate systems. Here is another complicating effect of the breadth and depth of ICT diffusion throughout advanced states and societies: many prosaic factors impede implementation of otherwise uncontroversial forms of defense.

More difficult challenges arise when activities could extend beyond the defender's networks and into those of others, including perhaps neutral parties, especially if a competent legal authority did not authorize such activities. Dorothy E. Denning and Bradley J. Strawser, in chapter 12, analogize such defensive cyber measures to air defenses. Taking down hostile botnets, for example, could be akin to taking active defenses against hijacked aircraft. Such measures can range from forcing hijackers to land at specified airports to, in the extreme, shooting down such aircraft in a scenario like the September 11 attacks on the United States. Defensive attacks "out of network," Denning and Strawser argue, should follow established principles of the laws of armed conflict that require necessity, discrimination, and proportionality. Their treatment of these issues, of course, is more nuanced than summary here allows, and the challenges deriving from uncertainties in the potential effects of cyber operations in external networks must figure prominently in the planning and conduct of defensive measures. One important question that will increasingly be raised is whether and under what conditions to allow, or even encourage, private businesses and other actors to conduct defensive measures. Here, too, governments nationally and internationally will need to refine relative distinctions between passive and active defensive measures and whether they operate within or outside of the defender's own networks, under what oversight, and to what effects.

Feaver and Geers explore issues of command and control and of the predelegation of authority to conduct defensive cyber operations. They note that as with nuclear weapons, cyber threats and operations feature great speed, surprise, and specialization on the part of those charged with planning and conducting responses to attack. Fortunately, thus far, "cyber weapons do not pose

an immediate, apocalyptic threat on the scale of nuclear weapons." This obviates the need always to be able and ready to retaliate quickly and therefore to establish pre-delegated authority. Indeed, thus far, most states, if not all, have demonstrated notable caution in authorizing even defensive cyber operations that could affect others' ICT. As we discuss later, this restraint stems in part from the difficulty of confidently attributing not only vectors of hostile action but also who authorized them, and from uncertainties over the intended and unintended effects of robust defensive actions. Moreover, the need for pre-delegation and for the automation of out-of-network defensive measures is attenuated by the likelihood that attacks on hostile botnets will require intricate sustained efforts to collect evidence and mobilize countervailing capabilities. Such time allows for the acquisition of court orders or other political-legal authority. Again, this distinguishes defensive cyber operations from nuclear defense and retaliation.

Still, cyber conflict remains a relatively new and rapidly evolving phenomenon. Artificial intelligence capabilities are developing quickly, as is the effort to leverage them into autonomous fighting systems, including in cyberspace. Most states are wrestling with how to structure and authorize command and control of cyber operations. As various military and civilian services organized on functional and regional lines face cyber threats and develop cyber capabilities, leaders struggle to define who can conduct what kinds of operations and under what conditions. Feaver and Geers highlight that the pre-delegation of some types of operations may be useful, "but its parameters must be governed by the existing laws of war." However, within this general framework, to which not all states may adhere, many important and complex issues are yet unresolved.

Nonproliferation

Complementing efforts to defend against cyber attacks, states will naturally seek ways to prevent the proliferation of software (malware) that could be particularly threatening to the maintenance of social stability. Unfortunately, the diffusion of offensive cyber capabilities is proving hard to control or restrict either by new arms control agreements or by the expansion of export control regimes, especially the Wassenaar Arrangement of 1996. This is partly because cyber tools are almost always inherently dual use, with their civilian applications being quite valuable and widely supported. Verification of arms limitations, so germane to the arms control agreements of the Cold War era, is practically infeasible with cyber technology.

Resiliency

Because defenses against cyber intrusion and attack are not perfect, and the spread of offensive capabilities cannot be blocked with confidence, states and major private enterprises must invest in resiliency. Resiliency will mean and require different things in different contexts—that is, in the military, the financial sector, the energy sector, and so on. The general aims are to decentralize potential points of failure or loss, to deploy backup capabilities and plans, to

prepare users of systems for the possibility of disruption, and to plan contingencies accordingly. Of course, while resiliency may deny attackers the gains they seek, pursuing it runs counter to normal economic logic.

Controlling Proxies

Whether resiliency is embraced and implemented widely, limitations in the effectiveness of defenses and nonproliferation initiatives mean that a central challenge now is to narrow the range of threatening actors. Against the tide of globalization, states must affirm as fully as possible their position as the monopolistic controllers of the projections of force (including cyber force) from their territories and by their citizens abroad. The importance of this effort addresses the need to diminish room for cyber privateering to take place.

Florian Egloff aptly describes in chapter 14 the rise and fall of naval privateering between the fifteenth and seventeenth centuries, suggesting that we are currently at a somewhat analogous early stage in the cyber domain. Indeed, we may be in a stage reminiscent of the earlier phase of privateering, which saw a significant growth in the phenomenon's scope. There are various systemic and case-specific motivations for abetting cyber privateering, but one that deserves special attention is the rapid progress being made in attributing cyber attacks to their perpetrators. This progress, facilitated in large part by intelligence breakthroughs even more so than by cyber forensics, has the unfortunate side effect of encouraging states to privatize some of their offensive cyber operations. Herein lays the importance of codifying the sovereignty, the jurisdiction, and the responsibility of states in the cyber domain.

Deterrence and Compellence

Turning to more dynamic and fraught approaches to using cyber instruments to prevent or manage conflict, deterrence and compellence assume major importance. It should be emphasized that cyber instruments and operations could be used alone or in conjunction with other capabilities to affect a wide range of adversarial behavior beyond cyber attack, espionage, and thievery. The choice of instruments should depend on whom is to be influenced to eschew or desist from doing what. In this broader context, potential cyber operations can serve signaling purposes short of war. Indeed, such signaling is a feature of deterrence and coercion, or compellence. The aim is to signal a threat of future action and motivate the adversary to eschew or de-escalate violence or to otherwise change behavior.

Before considering what concepts, strategies, and tactics are most suitable to contest cyber and other threats today, it is helpful to recognize that the contemporary environment differs greatly from the Cold War period in which major states developed their national security strategies and instruments. The nature and frequency of confrontation in the contemporary world, especially in cyberspace, are quite different from the central challenge that deterrence addressed in the Cold War. During the Cold War, few said that illicit activities by mafias, terrorist acts by the Red Brigades of Italy, propaganda campaigns by major pow-

ers, or revolutionary conflicts in Southeast Asia, Africa, and South America were failures of deterrence. Commentators today, however, say that the Sony Pictures Entertainment attack, the hack of the US Democratic National Committee, and the takedown of the Ukrainian power grid represent failures of deterrence. Several dubious assumptions operate here. One is that deterrence is *the* appropriate lever to counter such a wide range of hostile actions. Another is that cyber capabilities and policies should be the primary tool for deterring any and all nefarious acts conducted by cyber means. As the eminent strategist Robert Jervis recently noted, "There is no such thing as cyber deterrence."[2] While this may well be an overstatement, the unique features of cyber capabilities—versatility, low cost, vast range, high speed, and difficulty of detection and attribution—can be used to support a wide range of national policies including deterrence and, more broadly, coercion to influence an extensive array of adversarial activities.

The use of cyber threats (and attacks) for deterrence and compellence of hostile cyber or other activities presents several nearly unique challenges. For a threat to be effective, the opponent needs to perceive it, but, as discussed previously, one attraction of cyber capabilities to date has been their secrecy. On the one hand, because cyber attacks remain generally anathema to much of the world, states perceive reputational risks in being exposed as active or potential attackers. On the other hand, as cyber weapons spread and cyber warfare becomes commonplace, actors may find secrecy unnecessary and unhelpful insofar as deterrence could be augmented by making their offensive capabilities better known. Further, if norms of behavior for the legitimate conduct of cyber conflict are developed, then states may become more transparent, at least regarding the types of operations that could be justified under such norms and be consistent with rules of armed conflict. Of course, operational imperatives are another motivation for secrecy. States (and others) do not want to alert potential targets of possible types and methods of operations and thereby enable adversaries to take defensive measures that would erode offensive capabilities. The Snowden revelations are an example of both motives for secrecy: the United States suffered reputational damage, and the revelations helped competitors to defend against US techniques. Whether effectiveness of deterrent threats requires an opponent to perceive in some detail what harm can be inflicted on it or, instead, whether a vague sense of possibilities is sufficient for deterrence remains speculative.

Of course, it is possible, and perhaps likely, that revelations (such as Snowden's) of capabilities and attacks that have already occurred give other states and nonstate actors a sense of what can be done and thereby create a general basis for future deterrence and compellence. Any group contesting a state with demonstrable capabilities such as the Stuxnet operation against Iran, the reported Israeli corruption of Syria's air defenses, the Chinese penetration of US government and health insurer files, and the Russian hack into the US Democratic National Committee files should anticipate that similar actions can be taken against it.

Looking ahead, for deterrence and compellence to be effective, the issuer of such threats needs to have not only credible capabilities but also plans to win, or

at least not to lose, an escalatory process if the adversary does not relent. Yet, to date, there is no consensus on the meaning of "escalation" with cyber instruments. Uncertainties surround the potential effects of many possible cyber moves. The inability to distinguish computer network exploitation from computer network attack is fundamental in this regard. In crises or early stages of mobilization toward armed conflict, states that detect adversarial penetrations of their networks may find it difficult to assess whether the intentions are to gather intelligence or to conduct an attack—or both. They will prudentially assume the worst. More broadly, as Robert Jervis notes, "one could not know the physical, let alone the psychological and political impact, of exercising various cyber options; the country that is the object of the attack would assume that any effect was intended."[3] This situation can stimulate preemptive attack or other forms of escalation.

States (and other actors) will simultaneously seek to prepare for escalation and to minimize the risk. There is great tension between the two imperatives. Preparing the "battlefield" could advantage one or all parties to a potential conflict and could perhaps augment deterrence by motivating the adversary to back down. Conversely, it could lead to escalation, whether desired by one or both parties or not.

The tension between secrecy and deterrence exacerbates this conundrum. Revealing that one has penetrated or can penetrate various networks and do discrete kinds of harm can bolster deterrent or compellent threats. Such displays, however, weaken the weapon. For military operational purposes, as distinct from deterrence, one wants the adversary to *underestimate* its vulnerabilities and the threat one poses to it.

For these and other reasons, calculating whether and how deterrence and compellence by threats of cyber punishment can work is difficult. As Steven E. Miller and others note, the number and types of actors and scenarios that need to be deterred and compelled in the cyber domain are large. Moreover, attributing who is responsible for acts that would warrant retaliatory attack is fraught with technical, legal, and political difficulties, which would obtain even if the conductor of deterrence and compellence threats was entirely certain of the effects its potential attack(s) would have. Similar concerns likely would or should affect strategies to use offensive cyber attacks to limit the damage adversaries otherwise might threaten to inflict by cyber or other means—that is, deterrence by denial as distinct from deterrence by retaliation.

A number of these considerations are addressed in this volume. Three additional issues deserve mention here.

First, compellence is inherently more difficult to achieve than deterrence is. States that have committed national prestige and considerable resources to pursue fundamental objectives are highly resistant to external pressures to desist. It is easier to deter actors from doing things they are not already doing. The Stuxnet attack on Iran is perhaps the leading, if not only, example of a cyber operation that appears to have helped motivate a determined state to halt a threatening

activity it was already conducting. Further research should be devoted to seeking examples wherein cyber threats and actions have compelled adversaries to abandon hostile behavior, whether such behavior is cyber related or not.

Second, the development of effective cyber defenses and hardening to cyber attack could significantly bolster cyber deterrence and compellence. A blend of robust offensive and defensive capabilities could make a state's deterrent and compellent threats against an adversary more credible by lessening the adversary's probability of retaliating effectively. It could also mitigate risks of escalation. However, if one or more adversarial groups of states achieved defensive capabilities that made their offensive threats more credible, would this enhance stability or more likely fuel the equivalent of arms racing and crisis instability?

Third, it is an open question whether offensive cyber capabilities are more or less strategically valuable for weaker parties than they are for stronger ones. States with greater capabilities are likely to be more vulnerable and sensitive to disruptions in cyberspace that could affect them directly or could emerge as blowback from their own cyber operations. Weaker actors, whose coercive capabilities, societies, and economies are less digitally dependent, may feel they have relatively less to lose in cyber conflict. The Pearl Harbor analogy suggests that weaker parties may see comparatively less risk in conducting cyber attacks, though in the end the stronger party prevailed, while Lambert's chapter on British economic warfare illustrates the risk of blowback from a stronger party's use of economic warfare.

The Potential for Restraint

Finally, as experience with cyber conflict is thus far rather limited, any state contemplating major attack—as part of a strategy of deterrence, compellence, or preemptive use of force—will create a precedent that could open the way for others to follow suit. There may be advantages to being the first mover—as, for example, the United States felt in the use of nuclear weapons against Japan and the use of Stuxnet and its predecessors—but the first move is rarely the last one. An actor's relatively easy entry into the world of cyber conflict practically ensures that once the actor gains significant advantage from a type of attack, others will be inclined to do something similar. Notwithstanding the great uncertainty about the future of cyber conflict, several dynamics currently seem clear enough: First, offensive cyber operations are on the rise in terms of both intensity and frequency. Second, capabilities to undertake far bigger attacks than have occurred to date are already in the hands of several states. Their ranks are growing. Third, the possessors of strategic cyber capabilities, even those employing offensive cyber operations regularly, still consciously refrain from exercising them to the utmost, regardless of how otherwise appealing the use of these weapons might appear. This pattern of caution on high-end uses holds true even for states that otherwise challenge the status quo.

Historical analogies and our preceding analysis prompt us to speculate what could be the reasons for such restraint, even if considerations vary among the

actors that possess the pertinent capabilities. The following factors, which we do not attempt to weight or ascribe to particular actors, may help explain the apparent moderation of offensive cyber operations to date.

- Ethical considerations and legal concerns related to the laws of armed conflict clearly are one factor, even if less obviously reflected by Russia. Even in the shadowy cyber world, where few formal rules apply, most countries deem certain activities to be extremely unethical if not altogether illegal.
- Vulnerability to retaliation by cyber means seems to be another prominent concern insofar as some of the leading possessors of cyber armory are also heavily dependent on ICT for their prosperity and strength.
- Duality of intelligence and offensive cyber resources and opportunities discourages the use of offensive cyber tools for fear of compromising or burning unique intelligence assets.
- Uncertainty about the identity and affiliations of real sponsors of cyber aggression, as well as reluctance to divulge sources and methods that have made attribution possible, could explain inhibitions to undertake retaliatory cyber attacks.
- Considerations of efficacy, and the possibilities that cyber weapons could underperform or over-perform, seem to inspire restraint. This seems especially pronounced when contemplating attacks that might have strategic consequences. Some persistent and profound concerns are that cyber offensives might fail to achieve the objective assigned to them, that their perpetrators might be exposed, and that the attacks could produce unintended consequences including extensive collateral harm and damage bordering on the effects of using weapons of mass destruction. A particularly prominent concern with cyber weapons, analogous perhaps only to the massive use of nuclear weapons, is the possibility that their adverse consequences would not only affect noncombatants in adversaries' territories but could also seriously undermine the entire human habitat or its commercial lifeline, thereby also gravely harming the interests of the perpetrator.
- Growing concerns are that the employment of offensive cyber tools might not only incentivize others to use similar tools against highly sensitive targets but also provide adversaries the capability to reverse engineer these tools.
- Recognition that, once used and detected, cyber capabilities likely will not be usable again creates a "use only in extreme emergency" mentality.

Obviously these constraints are not of equal weight and effect on particular states (such as Russia). We are also at an early stage in the practice and study of offensive cyber operations and conflict. The observations, analyses, and speculations we offer here are meant to stimulate further analysis and debate, drawing on pertinent analogies from the past, and help scholars and practitioners to shape the future.

Notes

1. Gregory D. Koblentz and Brian M. Mazanec, "Viral Warfare: The Security Implications of Cyber and Biological Weapons," *Comparative Strategy* 32, no. 5 (2013): 418–34, DOI: 10.1080/01495933.2013.821845.

2. Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (Spring 2016).

3. Ibid., 70.