Cyberwar Thresholds and Effects

This article reviews cyberattack in armed conflicts, thresholds for considering cyberexploits as a use of force, existing armed conflict laws' applicability to cyberattack, and the political implications of cyberexploits' strategic versus tactical applications.

James A. Lewis
Center for Strategic and International Studies

The use of cyberattack in armed conflict is inevitable, but we need a clearer view of what cyberwar will look like, and how and under what circumstances militaries will use cyberattack. A broad range of malicious actions in cyberspace is routinely described as *cyberwar*. The identity of those who engage in these actions can be uncertain, and their intent is often ambiguous. However, this uncertainty doesn't justify a similar imprecision in describing cyberconflict. Imprecise terminology hampers serious discussion—it's unhelpful and incorrect to call every bad thing that happens on the Internet a "war" or "attack." The thresholds for war or attack in cyberspace shouldn't differ much from those in physical activity.

We can reduce this imprecision by disaggregating the different kinds of malicious cyberactivities and defining probable outcomes more carefully. Questions about the nature of cyberwar and cyberconflict reflect, to a considerable degree, weak data, vague terminology, and a certain reluctance to abandon the notion that cyberconflict is *sui generis*, rather than another new technology applied to warfare. To refine discussion, I define *cyberwar* as the use of cybertechniques to cause damage, destruction, or casualties for political effect by states or political groups. A *cyberattack* is an individual act intended to cause damage, destruction, or casualties.

Violence—or the threat of it—requires the use of force. Force involves physical harm or intimidation (the threat of physical harm). Warfare is the use of force for political purposes. These concepts provide thresholds for deciding when an instance in cyberspace is an attack, warfare, or the use of force that could justify the use of force in response. If the event doesn't involve violence or the threat of violence, it is not an attack.

In making this distinction, it's important to differentiate between covert actions that entail the use of force or violence, and espionage aimed at the illicit collection of information. This is an area for potential misperception in cyberconflict. Discovering that your network has been penetrated could be intimidating. However, if an opponent intends for a cyberexploit to be undetected, and if the exploit doesn't inflict physical damage or destruction, it's not intimidation, the use of force, or an attack.

Of course, there's a gray area when we think about disruption, particularly the disruption of services and data and when this disruption rises to the level of use of force. A denial-of-service attack, such as those launched against Estonia, wouldn't be considered an attack unless it was extensive and prolonged, having essentially the same effect as a naval blockade on the target country's commerce (an idea first proposed by Jaak Aaviksoo when he was Estonia's Minister of Defense).

This article focuses on the use of the Internet for armed conflict and predicts what cyberwar really looks like, reviews the utility and use of cyberattack, and considers nation-states' and other armed groups' likely behavior in waging cyberwar.

Technology and Weapons

We can benefit from putting cyberwar in the context

 1540-7993/11/$26.00 © 2011 IEEE COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES

of military technology changes and the resultant strategy and doctrine developments. The weapons and tactics the Duke of Wellington used in 1814 weren't markedly different from those the Duke of Marlborough used in 1704, more than a century earlier. One noted military historian goes as far as saying that Wellington's weapons and tactics didn't differ greatly from those used by Alexander the Great.[1] Technological change—the product of industrialization, mass production, and the expansion of science—transformed warfare. By the end of World War I, the ability to create new technologies and exploit them for military benefit had become an essential part of conflict.

We can regard the Internet as the latest development in military innovation. The expansion of command and control and the reduction of the uncertainty that creates the Clausewitzian "fog of war"—the uncertainty and confusion that hampers commanders during battle—changed how wars are fought.[2] We know from experience that a networked force is more effective than a non-networked force of similar size. Networked air defense is appreciably more effective than an aggregation of individual units. Nation-states with armored vehicles, aircraft, and ships connected by data links will fight more effectively than their counterparts who rely solely on voice. This increase in effectiveness makes military networks legitimate and valuable targets. Network technology use and cyberspace exploitation for intelligence and attack have become a normal part of military activity.

Cyber as a Weapon

Cyberwarfare will involve disruption of crucial network services and data, damage to critical infrastructure, and the creation of uncertainty and doubt among opposing commanders and political leaders. Cyberattacks let attackers strike both tactical and strategic targets from a distance using inexpensive systems. Although they're unlikely to be decisive and won't produce victory by themselves, particularly against a large and powerful opponent, cyberattacks offer a strategic advantage and will be part of future military planning and operations.

Cyberweapons can sometimes go beyond disrupting networks and inflict physical damage. For instance, during the Aurora tests at the Idaho National Labs, a remotely transmitted command caused an electrical generator to self-destruct.[3] These episodes suggest that cyberattack can be seen as another long-range strike weapon—faster than missiles or aircraft, not as destructive, but cheaper and possibly covert. Cyberattacks could have strategic or tactical application, depending on their target, with differing political implications for response, escalation, and international opinion. For these reasons, all major militaries have or are developing cyberattack capabilities. The most significant cyberpowers have developed and tested attack capabilities and routinely undertake the reconnaissance of targets necessary to carry out cyberattacks.

To understand cyberattack's role in war, we must ask the same questions we would ask of any other weapons system, such as what are the range, destructiveness, cost, effect, and political implications of its use? Cyberattack has both tactical and strategic applications. It can be used against deployed forces or strategic targets that contribute to an opponent's ability to wage war. Its range is practically unlimited, in that it can be used anywhere the global network extends. It has a variety of delivery options over networks or from dedicated platforms (ground, sea, air, space). Although the preparations for a cyberattack might be lengthy, the actual attack speed is measured in seconds, irrespective of the target's distance. The cost is relatively low, and surprise and stealth are normal attributes.

However, cyberattacks also have disadvantages. We don't yet have the ability to accurately estimate their potential collateral damage, particularly as a target set moves from tactical (such as deployed military forces) to strategic (such as civilian infrastructure). For attacks that disable networks, there could be unintended consequences not only to the target but also to noncombatants, neutrals, or even the attacker, depending on the interconnections of the target network or machine. This potential for unpredictable collateral damage increases political risk (for example, an attack on a Serbian network damages NATO allies' commercial activities) and carries with it the risk of escalating a conflict (an attack on North Korea damages services in China). This unpredictable collateral damage constrains nation-states' cyberattack use.

In this area, the similarity of cyberattack is similar to nuclear weapons. Strikes on deployed forces, apart from their military benefits, will create unease and concern over potential escalation. In contrast, striking civilian targets, including critical infrastructure, in an opponent's homeland could cause major conflict escalation; the target's reaction to these attacks would be pronounced. Attackers might intend to limit the attack's scope, but their opponent might not perceive (or believe) the limitations. Cyberattacks' uncertainty creates political risk—unexpected collateral damage can weaken international support, produce a negative domestic reaction, and stiffen resistance in the target country. In this sense, cyberattack is a tactical weapon with potential strategic consequences.

However, compared to other weapons, particularly strategic weapons, cyberattacks aren't very destructive. For all practical purposes, they're intangible, tiny electrical pulses whose destructiveness and lethality come not from their own innate destructive capac-

ity but from the ability to instruct tangible systems to malfunction. At this time, the possibility of damage, death, and destruction from cyberattack is low. An attack that causes a generator to self-destruct would do physical damage and might cause some casualties, but in general, these would be limited. For example, in 2009, a turbine in a Russian dam self-destructed because of operator error in remotely transmitted instructions. The result was reduced electrical production, flooding, and several casualties. Although this was a major accident, we do not want to inflate its military effect, which was trivial. Cyberattacks' physical consequences are more like sabotage carried out by guerrillas or Special Forces rather than a strategic weapon or attack and occupation by ground forces.

Military planners often target critical infrastructure to gain tactical or strategic advantage. Warsaw Pact planning in the Cold War targeted Western European power grids, telecommunications services, transportation hubs, fuel pipelines, and government centers. Disabling these targets would have contributed to the ground assault's speed and success. Cyberattacks could potentially provide the same disruption (and possibly make it easier for any occupying force to restore service). This is different from strategic attacks against government structures and manufacturing or other critical infrastructure in which the intent is not to gain immediate tactical advantage but to destroy or degrade the target's capacity for sustained resistance. A cyberattack's ability to dramatically erode the capacity to resist is open to question, but its ability to interfere with communications and logistics for tactical advantage isn't. For certain kinds of conflict, an opponent could reasonably be expected to use cyberattacks to interfere with efforts to move and supply forces.

Cyberattacks on hospitals could easily produce casualties by manipulating data, changing prescriptions, or turning off life support or other critical systems. Although terrorists might find these kinds of attacks attractive, these would be contrary to the existing laws of war. Harming noncombatants is also unlikely to produce much military advantage. Attackers might still strike hospitals, similar to how ambulances and hospital ships end up as "inadvertent" targets. Attacks on critical infrastructure, such as the power grid, might also harm medical services and produce casualties, but they wouldn't be considered contrary to the laws of war if the target's value is deemed to outweigh the risk of noncombatant causalities and any subsequent political repercussions.

The effect of attacks on infrastructure is easy to overestimate. Again, cyberattacks will resemble those actions in which guerrillas blow up substations or pull down power pylons to remind the opposing government of their presence and to erode its legitimacy. Guerrillas don't expect to win as a result of these attacks. With the right leadership, large industrial nations can absorb many blows before their ability to wage war suffers. In fact, in some conflicts, many nation-states are reluctant to do too much damage to infrastructure on the grounds that they will soon rely on it. In state-versus-state conflict, the issues for attacks on peer/near-peer infrastructure are whether the risk of escalation outweighs the military benefit of disabling infrastructure, and in a large-state/small-state conflict, whether the damage will harm any effort at postconflict "nation building."

Utility of Cyberattack

One way to assess cyberweapons' utility is to ask whether any nation believes it gains coercive advantage from their possession or independent use. One concern held by both the US and the Soviets during the Cold War was that allowing the other side to gain nuclear superiority would encourage the opponent to engage in coercive behavior and, possibly, increase the likelihood of a surprise first strike. Cyber superiority bears a small resemblance to nuclear superiority, which threatened a disarming and disabling first strike. A cyber-first-strike is conceivable as part of a larger campaign, but a cyberstrike alone would serve only to warn and irritate an opponent. In this sense, cyberweapons don't carry the same heft as conventional or strategic forces. An opponent could threaten cyberattack as a coercive measure, but the threat's credibility would diminish rapidly if it wasn't carried out and the target took defensive measures. Given their limited capacity for damage, cyberattacks might depend more on speed and surprise to achieve an optimal effect.

However, cyberattacks introduce a new dimension in the ability to cause uncertainty—a large part of Clausewitz's fog of war. Uncertainty slows decision-making, amplifies caution and timidity, and increases the chance of error. Misleading an opposing commander has always been part of warfare. Cyberattack provides a new and more intimate capacity to undertake active measures to mislead, offering a significant advantage in deception and undermining confidence. For example, the Allies went to great lengths to deceive the Germans as to where they would land in Operation Overlord (the invasion of Europe) by creating dummy armies and planting false information. The Germans might have hesitated to commit armored reserves against the Normandy landings because they were unsure whether these were a feint. Ultra—the British program to compromise encrypted radio communications that the Germans believed were secure—is a classic signals intelligence coup. The Allies enjoyed sizable operational benefits, particularly because the Germans didn't suspect that they were penetrated.

Cyberespionage could produce a similar advantage today. However, this is espionage rather than attack.

Cyberattack provides advanced militaries much greater capabilities for confusion and doubt than Ultra provided the Allies. Whereas Ultra was a passive collection technique, cyberattack interferes with command and control, providing attackers not only intelligence but also the ability to disrupt. A cyberexploit that can surreptitiously manipulate data in ways unfavorable to the opposing commander provides a new dimension for cyberconflict. In addition, attackers could let the targets discover some cyberefforts to create distrust and hesitancy. The Iraqis were hampered by a fear that using their communications networks during Desert Storm would expose them to American signals intelligence. This slowed and complicated their decision-making.

The 2007 Israeli air strike attack on an alleged Syrian nuclear facility illustrates another kind of manipulation. The strike was reportedly accompanied by cyberattack in which the Israelis, perhaps using a mobile platform, manipulated Syrian defense radars to show the situation as normal.[4] Instead of a noisy jamming attack that would have alerted the Syrians, air defense radar screens showed the airspace as empty and peaceful, preserving the element of surprise. Astute attackers will use cybertechniques to not only better understand opponents but also degrade the warning and response.

Often, cyberintrusions can degrade morale and the will to resist. Estonian and Georgian political leaders felt pressed by Russian cyberintrusions; however, in the case of Estonia, the intrusions probably did more to increase resistance than degrade it. During the second Gulf War, American forces sent Iraqi commanders emails urging them not to resist and providing instructions on how to surrender, which affected Iraqi resistance. A well-designed program, perhaps using spoofed messages on social networks, could become a source of damaging "rumint"—intelligence based on rumors. For instance, in the 1980s, East German reservists received a message ordering them all to report in uniform and assemble one Saturday. The bogus order created confusion and annoyance, and perhaps provided some intelligence benefit. It's not hard to imagine some kinds of cyberattacks interfering with logistics chains, rerouting supplies or making it appear that there are shortages or surpluses when the opposite is the case.

These incidents illustrate how cyberattacks can increase military advantage. But cyberattack capabilities won't be decisive in the same sense as strategic weapons or main force convention attacks. Instead, they will contribute to friction that slows, distracts, and perhaps weakens a target's response. French Resistance attacks on transportation systems during the battle of Normandy are an example of this. By themselves, they weren't sufficient to produce victory, but they provided an advantage at little cost to the Allied forces. Similarly, cyberattacks can degrade the target's effectiveness by some degree that will provide advantage but by themselves won't ensure defeat.

Conflict Duration

One issue that has received insufficient attention is cyberweapons' life cycle. Whenever a new military technology is introduced, the possessor gains an immediate advantage. This advantage declines as the opponent adjusts and develops countermeasures. In a long conflict between advanced opponents, this technological back and forth can be pronounced. Cyberattack techniques, however, often depend on a hitherto undiscovered vulnerability in software or network configurations. Once the attack is discovered, the target can develop countermeasures that could significantly degrade the technique's value. Cyberweapons can be single-use attacks, and attackers might have to build entirely new tools after an initial success.

The conflict's scope and length are key determinants of the degree of military advantage the cyberattack provides. Cyberattacks will be more valuable in short conflicts. In conflicts limited in time and scope, the disruption cyberattacks create in services and logistics might provide an initial advantage and decline in utility as the target nation-state adjusts. In contrast, attacks against command and control, such as those that disrupt data and undermine confidence, could have a sustained, cumulative effect and increasingly hamper the ability to resist.

This calculus could change if cyberattacks damage industrial chokepoints, specific targets that would hamstring the ability to supply or support forces. The theory is sound, but it's easy to overestimate the ability to identify the full range of such targets, attack them effectively, and prevent the target from compensating for losses, particularly for large industrialized countries. An industrialized country with adequate political will can resist and respond for a prolonged period. The cyber equivalent of the 1943 Schweinfurt ball bearing raids, which used air strikes in an unsuccessful attempt to cripple the production of new weapons by targeting an industrial chokepoint, wouldn't be accompanied by heavy losses. But it would likely be no more effective in degrading industrial performance to a level that provided military benefit.

Attacks on infrastructure will have only a minimal effect in short "go-with-what-you've-got" wars. The target nation's industrial capacity and the production of new weapons will be less important in these wars. We won't be fighting industrial-era wars of attrition

between large regular forces that last for years. Attackers could successfully disrupt critical infrastructure, and—if the target nation's leadership manages the political implications of this—see little or no effect on the targets' military capacity. A disruption of industrial capacity takes time to translate into a degradation of effectiveness in field forces. Attacks must be cumulative and persistent to overcome opponent resilience and response. A short war could be over before cyberattacks on critical infrastructure provide significant advantage.

These factors suggest that a cyberattack independent of a larger armed conflict is unlikely. There are remarkably few instances of one nation engaging in covert sabotage attacks against another nation—particularly against a larger power—unless it was seeking to provoke or if conflict was imminent. The political threshold for cyberattack (as opposed to espionage) by a nation-state is likely to be as high as the threshold for conventional military attacks.

Scenarios for Cyberwar

We must consider different cyberattack scenarios to assess their probability and effect. Currently, the most probable scenario is a limited conflict between the US and Russia or the US and China, in which opponents would disrupt command and control, logistics, and other services for theater forces. Attackers could disrupt rear support services—bases external to the conflict zone, including in the US—but they might be reluctant to move from military targets to domestic civilian targets. Attackers would probably avoid strikes on critical infrastructure in the US homeland because of the risk of escalation, unless they were *in extremis*, in which case the risk might be outweighed by some other factor—for example, popular discontent with China's leadership over the conduct of the war. The tactical use of cyberattack in these conflicts is certain, but a decision to move from the tactical to strategic application of cyberattacks holds political risk. An opponent could interpret these strategic strikes as conflict escalation, justifying an escalated response, or they could affect international political opinion in ways unfavorable to the attacker.

Eventually, when regional powers such as Iran or North Korea acquire cyberattack capabilities (and this might not be as far off as we assume), a strike against civilian targets in the US homeland will be more likely. Cyber capabilities will give these nations a strategic response. Should US forces strike targets in their countries, they would feel little or no constraint in using cyberweapons to attack US targets. Iran and North Korea haven't hesitated to use kinetic weapons, and our assumptions about deterrence might not make any sense when applied to these countries. Their calculus for deciding to attack is based on a different perception of risks and rewards. What deters China or Russia might not deter Iran or North Korea. This alone makes a one-size-fits-all deterrent strategy for cyberconflict of dubious value.

Two interesting scenarios involve smaller states and insurgents. The first is whether a small state under attack by a large state would perceive any political constraint from launching cyberstrikes against the attacking power, particularly if the attack posed an existential threat. The second is whether insurgent groups will be constrained once they acquire a long-range attack capability. The US was able to attack Iraq with impunity. If the Iraqis had cyberweapons, would they have felt unconstrained in using them against the US homeland? These wouldn't have changed the outcome of the invasion but would have provided a degree of vengeance and increased the cost to the US. Similarly, the Taliban in Afghanistan or the Shabab in Somalia must fight in their own territory with little chance of attacking the US homeland. The increased potential for cyberattack as small countries acquire the capability to strike distant targets also applies to nonstate opponents, and in a world of inadequate cyberdefenses, cyberdisruptions for political purposes and even cyberattacks intended to damage or destroy could become routine.

Of course, many considerations other than the simple acquisition of cyberattack capabilities will shape small states' or insurgents' ability to use cyberattack. Although the tools are cheap, cyberattack is expensive because it depends on network target reconnaissance to find vulnerabilities. This reconnaissance must be periodically refreshed as networks change, add new equipment or software, or are reconfigured. A small nation or insurgent group that is plugged in to the cyberunderworld might be able to access such information or hire mercenaries. The key elements of cyberattack capabilities are preparation and a fast "refresh cycle" for targeting. Designing and managing a large-scale attack might still be beyond their capacity, but harassment attacks against specific targets—Washington, DC, for example—would be possible. As digital network applications and processing capabilities continue to expand, there might be commercial services and programs that can adapt to provide small groups with the necessary reconnaissance and planning capabilities.

Applying the Laws of War and Armed Conflict

If cyber is a new military technology, an immediate issue is to determine the applicability of existing laws of armed conflict to its use. This cursory review of scenarios suggests that the existing laws for armed conflict developed for kinetic weapons can be applied

to cyberattack. We must consider the principles of distinction, proportionality, and discriminate attack to the same extent for cyberweapons as we would for any other form of attack. However, areas of ambiguity exist, including violation of third-party sovereignty, terrorist cyberattacks, and the amount and nature of damage from cyberattack that could be interpreted as an act of war.

Some operational requirements, such as the degree of prior assessment of collateral damage required to make an attack consistent with the law of war, are also unclear. Attackers are supposed to consider whether attacks on civilian targets, such as infrastructure, are legitimate. This decision requires assessing whether the attack is "demanded by the necessities of war," whether resultant disruption or destruction would produce a meaningful military advantage, and whether incidental civilian casualties or damage to civilian property would exceed that needed to obtain a military advantage.[5] Such decisions are arbitrary and depend on judgment. Insurgents and terrorists won't likely be burdened by these concerns. And experience shows that the longer a war continues, the more flexible and encompassing the interpretation of acceptable civilian damage tends to become. Western nations, which tend to have (at least initially) a greater regard for the rule of law, might be more hampered by these principles when conducting cyberoperations, although all attackers must consider the effect of indiscriminate attacks on world opinion and on the eventual political conflict settlement.

The most important ambiguity is the threshold for regarding a cyberincident as the use of force. Under international law, use of force triggers the right to self-defense. This makes the question of the threshold between an act that justifies the use of force in response (an act of war) and one that doesn't a central part of cyberwar discussions. An act of war is the threat or use of force against territorial integrity or political independence. This threshold is by no means precise and leaves considerable room for judgment. Although some consensus is based on international practice that certain actions, espionage, crime, and propaganda don't justify the use of force in response, other areas aren't so clear. When does a cyberreconnaissance become an act of war? Reconnaissance by itself isn't usually considered sufficient justification, but reconnaissance that involved leaving behind a weapon, such as a submarine reconnaissance of a harbor that left seabed mines in place, could be interpreted as an act of war.

Violation of sovereignty is an imprecise guide for determining acts of war in cyberspace. Hackers, spies, and criminals routinely send packets across borders with malicious intent. These actions are violations of sovereignty, but individually, they don't qualify as acts of war. Inserting a spy, whether physically or digitally, wouldn't generally be regarded as a use of force justifying a forceful response, unless the violation could be portrayed as an attempt at coercion or intimidation. Some could argue that massive and repeated violations of sovereignty by cyberintrusion could be interpreted as an act of war and justify the use of force in response, but it would be incumbent on the target nation to first notify the attacker that further intrusion would be regarded as an act of war. The failure of any nation to make this notification or complaint in the face of the massive cyberintrusions over the last decade means that we have not taken the opportunity to create a threshold (and perhaps a constraint) in cyberconflict.

Ultimately, deciding whether something is an act of war is political, particularly in cases that fall in the gray area between irritations and actions that threaten the state's existence. For instance, the 1968 *Pueblo* incident—in which North Korea seized a US Navy intelligence ship on the high seas, killing some crew members and imprisoning the rest—involved force, violence, damage, and the violation of international law. It violated US sovereignty, but a response would have been costly. The attack didn't threaten the existence of the US and was ultimately interpreted not be an act of war. Two hundred and fifty years earlier, Britain began a war with Spain after the Spanish coast guard removed a British merchant captain's ear while looting his ship (the War of Jenkins' Ear). Although Jenkins' suffering was no doubt acute, it didn't compare to the harm inflicted on the *Pueblo* and its crew. Destruction or casualties justify going to political leaders to ask for a decision but don't determine what that decision will be.

Data and network disruptions, which are a form of physical destruction, could be considered an act of war, but we would need to consider the damaged data's scale and sensitivity. The author of a hostile act might also affect the decision to deem an attack an act of war. When a deranged English activist defaced unclassified Pentagon websites and damaged networks in protest against the Iraq War, this was considered a crime, not an act of war. If a state had been involved, the action would move closer to the act-of-war threshold. If a proxy was involved, and if the state sponsorship of the proxy could be established, it would also move closer to the use-of-force threshold.

This threshold question is important for decisions regarding collective defense. The exploits against Estonia, for example, didn't trigger the formal commitment under NATO's Article 5, in which an armed attack against one is considered an armed attack against all.[6] Article 5 and its emphasis on the use of force has shaped Western attitudes on warfare and

defense for 60 years, and NATO nations will need to carefully consider how to extend its application to cyberspace. The attacks on Estonia were intended to intimidate and punish but not to create damage. Lowering the threshold so Estonia-like incidents qualify as the use of force could have some deterrent effect against state opponents, but it could also be destabilizing, as many nonstate groups and even individuals could launch similar denial-of-service exploits (but nothing more damaging), and a forceful reaction by defenders, even against the right target, could result in overreaction and increased tension.

The emerging consensus is that a cyberspace attack produces the equivalent effect of an armed attack using physical means. If an incident doesn't produce damage, destruction, or casualties, it's not an attack. A gray area exists when deciding when the disruption of services and data rises to the level of damage or destruction equivalent to the use of force, but the simplest approach is to reason by analogy and ask whether the cyberincident creates damage equal to a kinetic attack. An effects-based definition sets a clear threshold.

Some NATO members would prefer to use Article 4 of the treaty for cyberincidents, which commits members to consult when their "territorial integrity, political independence or security" is threatened.[6] Members would decide whether a cyberincident rose to the threshold of an armed attack and develop an appropriate response. The dilemma with relying on Article 4 is that it weakens the ability to signal redlines or thresholds. In cyberspace, where malicious activity is a daily occurrence and collective defense isn't likely to deter incidents such as crime, espionage, and reconnaissance, ambiguity in the use-of-force threshold might lead attackers to underestimate the risk that their action will lead to an armed response and escalate conflict. The policy issue is to determine where ambiguity about a response to a cyberincident is beneficial and where it increases risk.

This brief review suggests that when considering cyberwar or cyberattack, we can place these actions into the existing framework of conflict and regard cyber in the larger political framework that governs conflict by assessing its effects and considering its consequences. This consideration will resolve around two thresholds that shape cyberconflict strategy and doctrine: the threshold for considering a cyberevent an act of war or use of force and the threshold between cyberattacks' tactical and strategic application. The analysis of when cyberevents cross these thresholds will determine their use and the response to their use.

Generally accepted international norms regarding cyberattacks' use would help define these thresholds. The development of such norms will require resolving ambiguities about cyberoperations' nature and effect. Many nations' unwillingness to admit that they have offensive cyber capabilities complicates the development of norms. Recent discussions in the UN, however, suggest that the international community (including the US, Russia, and China) are sufficiently concerned about the potential for inadvertent escalation as a result of cyberincidents that they will engage in creating norms and other confidence-building measures. The creation of norms—or at least a recognition of how existing norms for armed conflict apply to cyber—would reduce the imprecision and ambiguity that has marked this discussion. However, the interplay between norms, doctrine, and strategy deserves a separate discussion.

Digital networks are a new tool for state power, and cyberattack will be part of future military conflict. Like earlier technological innovations, it will reshape warfare. Unfortunately, some of the issues and ambiguities identified in this article won't be resolved until we gain more direct cyberwarfare experience. In the interim, war games and exercises can provide insights. Dialogue with both potential opponents and allies can begin to clarify issues and perhaps reduce the chance of miscalculation or misperception. Additional studies could also help define cyberwar and provide guidance on the use of cyberattacks, their risks, and potential responses. □

References

1. J. Keegan, *A History of Warfare*, Vintage Books, 1994.
2. C. von Clausewitz, *On War*, M. Howard and P. Paret, eds., Princeton Univ. Press, 1976.
3. J. Meserve, "Mouse Click Could Plunge City into Darkness, Experts Say," CNN, 27 Sept. 2007; http://articles.cnn.com/2007-09-27/us/power.at.risk_1_generator-experiment-cnn?_s=PM:US.
4. R.A. Clarke and R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, HarperCollins, 2010.
5. Hague IV Annex, Article 23; www.icrc.org/ihl.nsf/WebART/195-200033?OpenDocument.
6. North Atlantic Treaty, NATO, 4 Apr. 1949; www.nato.int/cps/en/natolive/official_texts_17120.htm.

James A. Lewis *is a senior fellow and program director at the Center for Strategic and International Studies, where he writes about technology, security, and the international economy. His research interests include cybersecurity, innovation, economic change, and asymmetric warfare. Lewis has a PhD from the University of Chicago. Contact him at jalewis@csis.org.*