2009-04

Barriers to Entry: Are They Lower for Cyber Warfare?

Denning, Dorothy E.

Barriers to Entry:

By Dorothy E. Denning

Recently, I was contacted by a group of researchers studying cyber warfare. In reading their project description, I was struck by one of their premises: "Barriers for entry to conduct activities in cyberspace are lower than in any military domain." I thought, yes, this is the conventional wisdom, but is it really true? What about warfare on land? While it may require substantial resources to assemble an army and invade a foreign territory, it is not hard to shoot a gun, toss a grenade, or start a fire – all operations that take place on land. If these operations are considered too individualistic or simple minded to be called land warfare, then is it fair to call a common cyber attack, say a simple denial-of-service (DoS) attack against a public website, cyber warfare? If the DoS attack is considered to be a means of cyber warfare, is it fair to compare its entry requirements with those for a vastly more complex army invasion when the effects are dramatically different? The DoS attack may shut down a communication channel on the Internet for awhile, but the land invasion could result in the overthrow of a government or the seizure of territory.

Perhaps cyber attacks seem to have a lower barrier to entry because they are so commonplace. Moreover, many are simple to perform using "point and click" software tools and easy-to-follow scripts. Teenage "script kiddies" launch cyber attacks without understanding how the tools work or exactly what they do. But young people also join street gangs, and teens who are clueless about conducting DoS attacks shoot guns and mark gang territory with graffiti. Children who have never even heard of the Internet fight in war-torn areas in Africa, wielding weapons and killing other human beings. If one considers all the attacks that take place just on land – shootings, stabbings, beatings, muggings, robberies, arson, etc. etc., surely they are at least as frequent as those in cyberspace, and often as easy to perform.

Are They Lower for Cyber Warfare?

Photo courtesy US Department of Defense.

The objective of this essay is to explore the question of whether operations in cyberspace have a lower barrier to entry than operations in kinetic domains of warfare, especially land. To do this, two factors are considered: costs and effects. Costs reflect barriers to entry and cover everything needed to prepare for and carry out an operation. They include expenditures for weapons, training, tools, facilities, telecommunications, salaries, travel, and recruiting. They also include casualties and arrests that result from the operation. Effects are the outcomes of an operation and include deaths, property damage, financial losses, service disruptions, decisions made, and actions taken.

Costs, or barriers to entry, are then examined relative to their effects. In particular, an operation X in cyberspace is said to have a lower barrier to entry than an operation Y in another domain relative to effects Z if the costs of X are lower than those of Y in order to achieve Z. Stated another way, if a given effect can be achieved in cyberspace for a lower cost than in some other domain, then cyberspace has a lower barrier to entry for achieving that particular outcome.

The remainder of this essay examines costs and effects in greater depth, discusses the Estonian and Georgian cyber conflicts in terms of their barriers to entry, and draws some conclusions.

COSTS

There are several factors that contribute to a sense that the barriers to entry for cyber operations are lower than for other domains. These include remote execution, cheap and available weapons, easy-to-use weapons, low infrastructure costs, low risk to personnel, and perceived harmlessness. The following examines these factors and whether they always hold.

Remote execution. Cyber operations can be conducted remotely, even from the other side of the world. By comparison, kinetic operations generally require that personnel and equip-

ment be physically transported to the target area. This can be extremely costly, such as when armed forces are deployed to a foreign country. If borders must be crossed illegally, it also can be difficult and dangerous. However, there are exceptions to the general rule. A particular cyber operation could require a physical presence at the target site, for example, an accomplice with inside access to the target. Speed or reliability requirements could also preclude some remote attacks, such as from a site vulnerable to frequent network outages. In addition, there are kinetic operations such as the firing of long-range missiles that can be conducted remotely. Also, kinetic targets can be selected on the basis of their proximity, precluding the need to relocate persons and equipment. Instead of traveling to the US, for example, terrorists frequently attack US interests abroad, including embassies and military bases.

Cheap and available weapons. Cyber weapons are cheap and plentiful. Indeed, many are free, and most can be downloaded from the Web. Some cost money, but even then the price is likely to be well under $100,000. By comparison, many kinetic weapons, for example, fighter jets, aircraft carriers, and submarines, can run into the millions or even billions of dollars. Again, however, there are exceptions. Custom-built software can cost millions of dollars and take years to develop, while kinetic weapons such as matches, knives, and spray paint are cheap and readily available.

Easy-to-use weapons. Besides being inexpensive, many cyber weapons require little skill beyond that required to operate a computer and use the Internet. By comparison, members of armed services receive extensive training to effectively use kinetic weapons. But as with the other factors, the general rule breaks down when one takes into account complex cyber weapons that require advanced skills or simple kinetic weapons like knives and spray paint that can be used by anyone.

Low infrastructure costs. In general, cyber operations require little infrastructure in the way of facilities and equipment. Even if multiple people are involved, operations can be coordinated from a website, with participants accessing cyberspace from their residences and cyber cafés. In comparison, armed services generally require substantial infrastructure, including military bases, to sustain their activities. However, the generalities do not extend to complex, tightly coupled cyber operations that require a team of people operating within a shared facility or loosely coupled kinetic operations like riots that erupt with little supporting infrastructure.

Low risk to personnel. In general, the persons involved in a cyber operation may be less likely to be captured or killed than persons involved in a kinetic operation. In part, this is because it can be difficult to determine the source of a cyber attack, especially if the attack has used proxies and hopped through multiple machines. Even if the source can be determined, the persons involved may be protected from capture or arrest by international boundaries, especially if they are operating on behalf of or with approval from their host government. In comparison, soldiers on the ground, at sea, or in the air generally risk being the targets of a lethal counter-strike. However, those launching missiles from a remote location or dropping bombs from the air may be safer than cyber operators who are careless or up against a concerted effort to track them down.

Perceived harmlessness. Many cyber attacks such as web defacements and low-level DoS attacks are perceived to be relatively harmless. Nobody dies and damages are not usually permanent. Defaced websites are quickly restored and normal traffic flow resumed when DoS attacks stop. Consequently, there may be less psychological aversion to conducting a cyber attack than a kinetic one, especially one that employs lethal weapons. A 14-year-old hacker might have no qualms about defacing a website, but never shoot a gun or detonate a bomb that would kill people or destroy property. But as with the other generalities, there are exceptions. A cyber attack could be deadly, for example, by disrupting emergency 911 systems, while a kinetic operation such as a peaceful street demonstration could have little or no harmful effects.

EFFECTS

In order to fairly compare the barriers to entry of a cyber operation with a kinetic one, the two operations must have equivalent effects. However, the immediate effects of an operation in cyberspace look substantially different than in other domains. While cyber weapons destroy and block bits, kinetic weapons destroy property, kill people, and block

At the Cyber Command (Provisional) network center at Barksdale Air Force Base, La., Staff Sgts. Benjamin Lockwood (left) and Andrew Corriveau discuss operational status. (US Air Force photo/Lance Cheung)

physical pathways. Moreover, because bits can be replicated and restored, the effects in cyberspace may be short lived in contrast to the permanency of death and longer-term effects of property damage.

Despite these differences, it is possible to frame many effects in a generic form that is domain independent. Casting effects generically provides a means of formalizing what it means for operations is disparate domains to have comparable or equivalent effects. By way of analogy, a bowl of apples is not comparable to a bowl of oranges, but the two bowls of fruit can have comparable weights.

One generic metric that applies to both cyber and kinetic domains is financial losses. Another is disruptions of service. For example, cyber attacks have caused airline delays, halted train service, and shut down ATM machines – all effects that could be achieved with bombs or even just the threat of bombs.

Although most cyber attacks do not damage physical property or result in death, those that do can be compared with kinetic operations that produce equivalent damages. For example, a cyber attack against a water treatment system in Australia caused raw sewage overflows, which in turn caused environmental damage – something that also could have been achieved with toxic chemicals. Although cyber attacks have not yet killed anyone, it is not hard to postulate scenarios that do so, for example, attacks that cause extended power outages or planes to crash.

Operations across domains could also be compared in terms of decisions made and actions taken, for example, a decision to meet an adversary's demands. ISPs, for example, have removed content from websites they host in order to halt crippling DoS attacks from persons who objected to that content. An equivalent operation in physical space might be a protest outside a bookstore or library demanding that a particular book be removed from the shelves. At a state level, a country might agree to the terms of another state as the result of either a cyber or kinetic operation.

THE ESTONIAN AND GEORGIAN CYBER WARS

In late April 2007, Russian hackers began a prolonged cyber war against Estonia. Prompted by the moving of a Soviet-era memorial, the assault in cyberspace included DoS attacks that disrupted access to selected Estonian websites belonging to the government, banks, and the media. It also included web defacements and spamming of government e-mail accounts. The cyber strikes went on for weeks, although the vast majority of the DoS attacks lasted less than an hour and only 5.5% over ten hours. (1) Some of the DoS attacks leveraged large "botnets" of compromised computers, while others involved individual participants following a script that performed a "ping" attack against target websites. (2) The total cost to the assailants was nominal, as participants volunteered their time and computers. Attack tools were free, although fees might have been paid for some of the botnets. Coordination was minimal, generally taking place on web forums frequented by Russian hackers. The risks of being caught and punished were also low, although one hacker living in Estonia was identified and fined about $1,620. (3)

The immediate effects of the cyber war were loss of access to certain websites and government e-mail accounts. This in turn interfered with the ability of Estonians to make online banking transactions, especially from overseas, and to use their bank cards for purchases. I found no estimate of the total financial losses incurred from the assault, but one bank was said to have lost at least $1 million. (4) Overall, the losses likely ran well into the tens of millions of dollars, taking into account the service disruptions and the efforts to mitigate, stop, and recover from the attacks.

Could the effects of the Estonian cyber attacks have been achieved with kinetic weapons at a lower cost? In fact, the memorial relocation also sparked low-cost street protests, leading to one death and 150 injuries. (5) However, to fairly compare the cyber and street actions, we need a generic metric, say, total monetary damages. Although I have not seen estimates of financial losses for Estonia's street (or cy-

ber) riots, they are available for other events. The riots in Seattle that accompanied the World Trade Organization's meeting in 2000, for example, caused an estimated $20 million in property damage and lost sales to downtown businesses, plus at least $3 million in added city expenses to handle the conference. (6) These damages might be roughly comparable to those of Estonia's cyber and street riots, but it is hard to say.

Even if the effects of the cyber attacks against Estonia exceeded those of the street protests, it is not clear that a repeat attack in cyberspace would have as much impact. The country's cyber defenses have been improved, and a comparable attack today might be relatively minor, with effects substantially less than those of the street riots.

Compared to the Estonian cyber assault, the one against Georgia in August 2008, also attributed to Russian hackers, was much less damaging. One explanation is that because of Estonia, the Georgians were better prepared. Also, the attacks did not persist as long – a few days rather than weeks. In addition, Georgia is less dependent on cyberspace for banking and financial transactions, so the attacks would not have affected day-to-day business as much as in Estonia. For Georgia, the Russian military's invasion of its territory had a much greater impact.

CONCLUSIONS

There are few obstacles to engaging in low-level cyber warfare, particularly DoS attacks and web defacements. Participants can join from anywhere in the world; they need little in the way of weapons, skills, and infrastructure; chances are good they will not be caught or harmed; and they might have few reservations about participating in activity they view as relatively harmless. However, this does not imply that the barriers to entry for cyber warfare are lower than for other domains. There are also few obstacles to conducting many kinetic operations such as street protests, fist fights, and gang warfare.

The important question is whether equivalent effects can be achieved in cyberspace but at a lower cost. To do that, operations must be examined in terms of generic effects that apply across domains, for example, financial losses, service disruptions, casualties, or decisions made. Only then is it fair to compare costs, which measure barriers to entry. It might have been easier and cheaper for Russian activists to engage a cyber militia to attack Estonian websites than for Iraqi insurgents to engage armed militias to attack US forces and each other, but the Iraq violence has caused vastly more damage, including substantial loss of life.

When examined in terms of equivalent effects, the barriers to entry for cyber operations may, on average, be about the same as for kinetic operations. It does not take much to cause a few thousand dollars of damages in either domain. However, if the knowledge, skills, and disposition of individual participants are factored in, there are likely to be persons willing and able to inflict that damage through a cyber attack but not a kinetic one, and conversely. Someone may join a cyber militia who would never participate in a traditional militia, while someone else may be more attracted to guns and bombs than bits. Thus, rather than competing, the two domains of warfare may draw from different constituents and affect different targets.

Seen from this perspective, cyber warfare opens up a new form of warfare to people who otherwise might not participate. This is especially evident in al-Qa'ida's global jihad, which includes cyber jihadists who attack websites in addition to terrorists who plan and conduct deadly strikes. The barriers to entry for electronic jihad may be lower than for terrorism, but then the effects pale in comparison to the wanton death and destruction of terrorism.

For now, the effects of cyber attacks are relatively minor compared to what is achieved with armed forces, especially military operations that lead to the overthrow of governments, seizure of land, and human casualties. The discrepancy may narrow with more sophisticated cyber attacks that affect physical systems, but such attacks are likely to also have higher costs, raising the barriers to entry.

In the end, there will be different levels of cyber warfare, with low barriers to entry for the patriotic and activist hackers who just want to cause a bit of disruption, not unlike that caused by street demonstrations and other kinetic operations with low barriers to entry. The barriers to entry will be higher for militaries using cyber strikes to achieve national objectives, but whether they will be lower or higher than for kinetic strikes that produce comparable effects is difficult to say without examining the details of specific operations.

Dr. Dorothy E. Denning is Professor of Defense Analysis at the Naval Postgraduate School, where her current research and teaching encompasses the areas of conflict and cyberspace; trust, influence and networks; terrorism and crime; and information operations and security. She is author of Information Warfare and Security *and over 140 articles. She has previously worked at Georgetown University, Digital Equipment Corporation, SRI International, and Purdue University. Dr. Denning received the B.A. and M.A. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University.*

ENDNOTES

1) "Estonian DDoS – A Final Analysis," Heise Security, 31 May 2007.
2) Joshua Davis, "Web War I," Wired, September 2007.
3) "Estonia Convicts First 'Cyber-War' Hacker," AFP, 24 January 2008.
4) Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," The New York Times, 29 May 29 2007.
5) Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," Culture Mandala, 8:1, October 2008, pp. 28-90.
6) "WTO Protests Hit Seattle in the Pocketbook," CBC News, 6 January 2000.