17

ASSESSING CYBER WAR

Dorothy E. Denning

This chapter introduces a framework for assessing cyber war. The framework can be used to assess a war that takes place exclusively in cyberspace or to assess the cyber component of a war that cuts across multiple domains—for example, land, air, and cyber. It is written from the perspective of one country, say the United States, which is engaged in a cyber war with an adversary.

The framework provides for two types of assessments. The first, cyber battle damage assessment, is used to evaluate the effects of cyber operations to determine whether operational goals and benchmarks are met. The second, cyber strength, is used to determine the relative strength of our own cyber forces against those of the adversary so that we can estimate the likely success of planned and future cyber operations by ourselves and the adversary.

Although the framework might be applicable to all types of cyber operations, the focus here is on *cyber attacks*, defined by the National Institute of Standards and Technology (NIST) as attacks "via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[1] Note that under this definition, cyber espionage and intelligence collection, or what the US Department of Defense calls exploitations, are considered to be cyber attacks. However, the definition excludes influence and information operations that do not affect cyber resources.

The framework uses as its foundation risk assessment, which is an assessment of the risks to cyber systems, operations, and organizations from cyber attacks. The chapter describes the elements of risk assessment, using the NIST model as its basis. It then shows how risk assessment can be applied to assess cyber war. With the framework in place, the chapter then discusses some of the difficult issues and challenges that arise in cyber war assessment.

RISK ASSESSMENT

Risk assessment is the process of identifying, estimating, and prioritizing risks that arise from the operation of cyber systems. These risks can jeopardize cyber systems, individuals and organizations, and a nation as a whole.

Cyber risks are identified and evaluated in terms of threats, vulnerabilities, impacts, and likelihoods. *Threats* are events that can cause harm. Sources of threats can be either adversarial or non-adversarial, with the latter covering accidents and natural disasters. Here we are concerned primarily with adversarial sources, which can be individuals, groups, organizations, and nation-states and are characterized by capability, intent, and targeting. Cyber threats from adversarial sources correspond to events associated with cyber attacks. Threat events are described by the tactics, techniques, and procedures used—for example, cracking passwords to gain unauthorized access, sending links to malware in deceptive e-mail messages, exfiltrating data from a compromised computer to a drop site, or flooding a site with packets in a denial-of-service (DoS) attack.

Vulnerabilities are weaknesses that can be exploited by an adversary. They include flaws in technology (both hardware and software), the configuration and operation of cyber systems (e.g., failing to change default system passwords), user practices (e.g., clicking on malicious links), and business practices (e.g., failing to plan for contingencies and ensure continuity of services). They are examined in the context of predisposing conditions, including system architecture and cyber defenses in place.

Impacts are the effects or harms produced by threat events. They include harms that can result from unauthorized disclosure or theft of data from cyber systems and from tampering with or denying access to cyber systems. They include both effects to cyber systems (e.g., data deleted or systems down or corrupted) and effects to those who depend on them (e.g., inability to perform functions of organization).

Likelihoods are the chances that threats will be realized (attacks will be initiated and then succeed) and that harms will occur. Once threats, vulnerabilities, impacts, and likelihoods have been identified and evaluated, they are combined to determine risk. The result is an appraisal of the ability of the cyber systems and organizations under review to resist and withstand the identified cyber threats.

Risk assessment can be quantitative, qualitative, or something in between. With quantitative assessment, individual factors are given numerical values, say on a scale from 1 (lowest) to 10 (highest). With qualitative assessment, they are given categorical values, say ranging from very low to very high. An approach in between might assign numeric ranges to categories such as 1–2 for very low, 3–4 to low, 5–6 to medium, 7–8 to high, and 9–10 to very high.

The NIST's *Guide for Conducting Risk Assessments* (Special Publication 800–30) offers a model and guidance for conducting risk assessments.[2] The processes and approach described therein are intended to be consistent with the risk assessment standards of the International Organization for Standardization and the International Electrotechnical Commission. The NIST guidance includes sample tables for identifying and qualitatively assessing each of the individual risk factors. The table for adversarial threat events, for example, includes descriptions for more than eighty sample events associated with cyber attacks. In addition, the guidance offers a sample adversarial risk table for combining the factors to determine risk (see table 17.1). Each row of the table corresponds to a threat event in a potential cyber attack. The columns of the table describe the threat event; possible sources of the threat and an assessment of their capability, intent, and targeting; the relevance of the event; the vulnerabilities that could be exploited by the threat and an assessment of their severity; the likelihood of one or more sources initiating the cyber attack and then succeeding; the level of impact from the threat event; and finally risk as a combination of likelihood and impact.

The NIST risk assessment methodology can be applied across three levels: Tier 1, or the organizational level; Tier 2, or the mission-business process level; and Tier 3, the cyber systems level. The levels correspond roughly to strategic, operational, and tactical risks, respectively.

CYBER WAR ASSESSMENT

To assess cyber war, we need to be able to assess two things. First, we need to assess cyber battle damages—namely, the effects of cyber operations—to determine if the United States is meeting its operational goals or benchmarks. Second, we need to assess our relative cyber strength against that of the adversary to determine the likely success of planned and future cyber operations by ourselves and the adversary. The following describes how the concepts and factors used in risk assessment apply to these assessment efforts.

Cyber battle damages are the effects produced by cyber operations conducted by ourselves and our adversary. These effects can be direct or indirect

Table 17.1 Sample adversarial risk table

Column	Heading	Content
1	Threat event	Identify threat event
2	Threat sources	Identify threat sources that could initiate event
3	Capability	Assess threat source capability
4	Intent	Assess threat source intent
5	Targeting	Assess threat source targeting
6	Relevance	Determine relevance of threat event
7	Likelihood of attack initiation	Determine likelihood that a threat source initiates the threat event
8	Vulnerabilities and predisposing conditions	Identify vulnerabilities that could be exploited during threat events and conditions that could increase the likelihood of adverse impacts
9	Severity pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions
10	Likelihood initiated attack succeeds	Determine likelihood that an initiated threat event succeeds
11	Overall likelihood	Determine likelihood that threat event is initiated and succeeds
12	Level of impact	Determine adverse impact of threat event
13	Risk	Determine risk of threat event as combination of likelihood and impact

Source: Adapted from table 1-4 of NIST, *Guide for Conducting Risk Assessments*, Special Publication 800–30 (Gaithersburg MD: NIST, September 2012).

and correspond to the impacts used in risk assessment. The difference is that whereas risk assessment is concerned with the effects of *potential* cyber attacks, cyber battle damage assessment is concerned with the effects of *actual* cyber attacks. However, both deal with effects not only to cyber systems but also to the organizations that depend on them.

The effects on cyber systems can be expressed in terms of effects relating to data and effects relating to hardware and software. Effects relating to data include exfiltration of data, corruption and destruction of data, and insertion of false data. They might be measured in terms of bytes, records, files, or media. For example, they could be reported as 100 gigabytes of data exfiltrated, 250,000 customer records taken and posted online, 15 files corrupted, 1 website defaced, or the hard disks of 30,000 machines erased. Effects relating to hardware and software include corruption and destruction of hardware and software, injection of backdoors and other malicious software (malware), system takeovers (i.e., system under control of adversary), and system outages (e.g., system becomes inaccessible because of a DoS attack). They might be measured in terms of the number of systems or components affected or the length of outages or disruptions.

The effects of cyber attacks on organizations can be expressed in terms of operational effects, monetary losses, and reputational effects. Operational effects include the inability to perform certain functions or to provide certain services. In a warfare environment, examples would be the inability to provide logistical support, rely on air defenses, deploy computer-controlled weapons systems, execute command and control, communicate with forward-deployed troops, or access certain intelligence sources. They might be measured in terms of the scope or duration of operations effected.

Monetary losses include direct losses (e.g., from fraudulent money transfers) as well as costs associated with responding to and recovering from cyber attacks (e.g., restoring systems, changing passwords, installing software updates or new security products, and investigating incidents). Monetary losses may be less important to military organizations than losses to operational capability during war, but they are still important as they reduce the funds available for other products and services.

Reputational effects include lost stature, trust, and respect that can undermine military objectives and missions. During war, for example, human intelligence sources might refrain from providing further information after a system compromise exposes them to possible harm, or allied forces might be unwilling to share their intelligence data if they believe it will not be adequately protected. Reputational effects can be enduring, jeopardizing future operations.

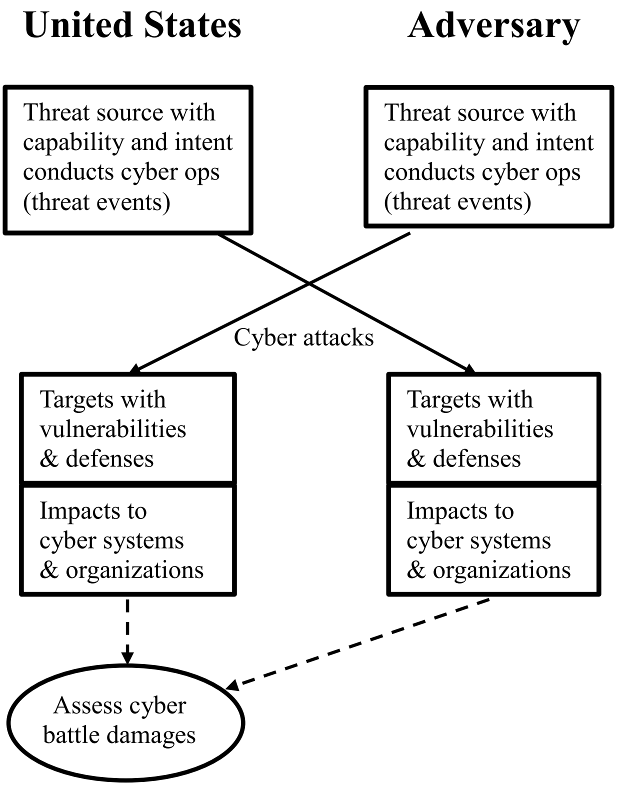

United States
Adversary
Threat source with capability and intent conducts cyber ops (threat events)
Threat source with capability and intent conducts cyber ops (threat events)
Cyber attacks
Targets with vulnerabilities & defenses
Impacts to cyber systems & organizations
Targets with vulnerabilities & defenses
Impacts to cyber systems & organizations
Assess cyber battle damages

Figure 17.1. Assessing cyber battle damages from US perspective

Note: Solid lines represent actual cyber attacks; dashed lines represent information flows for battle damage assessments.

We need to assess cyber battle damages inflicted on us as well as those inflicted on the adversary. In general, it will be easier to assess our own damages than those of the adversary, where our situational awareness is likely to be incomplete. However, we need to estimate the effects to their systems and organizations to know if we are meeting our operational goals and benchmarks in the cyber domain. Figure 17.1 illustrates.

Cyber strength refers to our relative advantage over the adversary in cyber war—that is, our ability to affect its cyber systems and operations versus its ability to likewise affect ours. To measure cyber strength, we need to consider more than the cyber capabilities of ourselves and the adversary. We also need to know whether our cyber operations are likely to succeed against the adversary and produce the desired effects, and conversely whether the adversary's operations are likely to succeed against us with their intended effects.

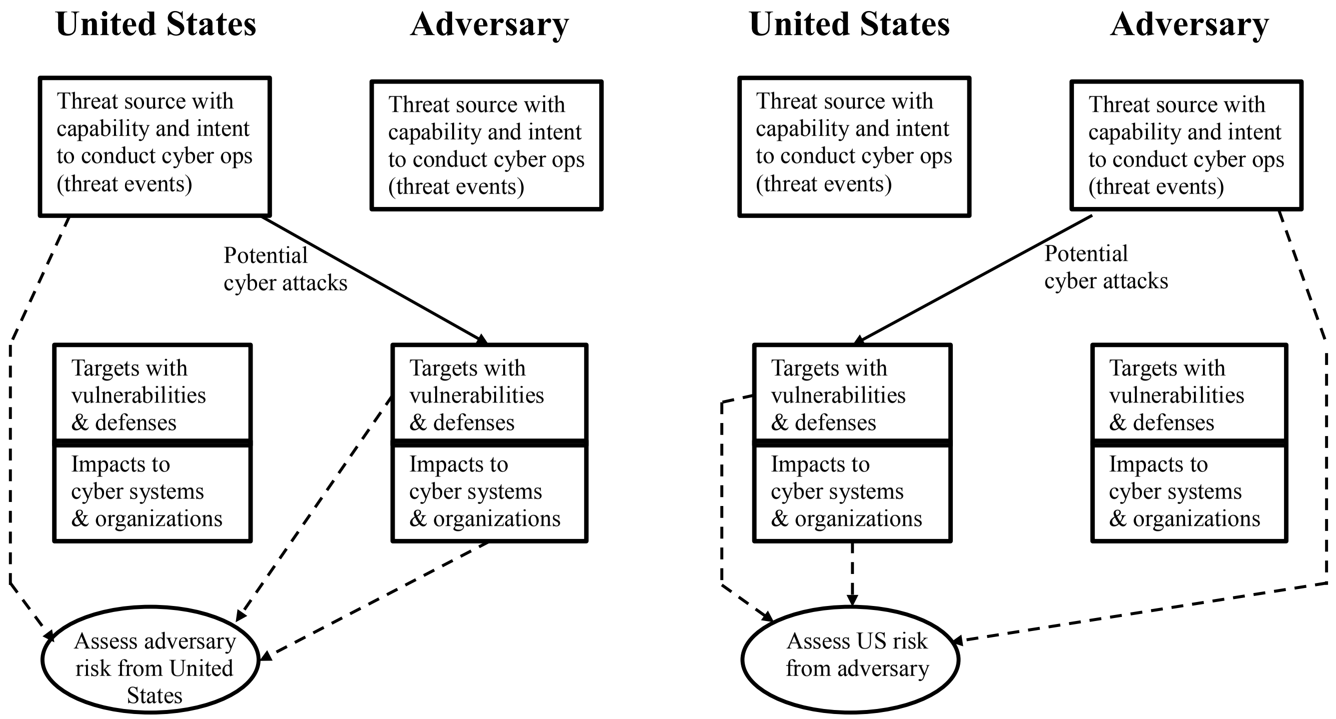
The only way to know if our cyber operations against the adversary will succeed is to factor in the adversary's vulnerabilities and defenses, and the only way to know what effects to expect is to add the impacts and likelihoods of success to the equation. This requires conducting a risk assessment of the adversary's systems while using ourselves as the threat source; that is, we need to consider the risk to the adversary of threat events caused by our cyber attacks. Even if our own capability is high, if the adversary either does not use cyber systems or has well-defended systems for functions we want to affect, our cyber capability will not afford an advantage. Likewise, the only way to know if the adversary's operations against us will succeed is to take into account our vulnerabilities, our defenses, and the impacts and likelihoods of its attacks. This requires conducting a risk assessment of our systems while using the adversary as the threat source. Only after undertaking these risk assessments will we know if our cyber operations and our adversary's are likely to succeed and create the desired effects. Figure 17.2 illustrates the process of assessing (a) their risk from our potential cyber attacks and (b) our risk from their potential cyber attacks.

Our cyber strength (CS) is then expressed as the ratio of the adversary's risk to ours, where its risk is determined using ourselves as a single threat source against it and where our risk is determined by using the adversary as a single threat source against us. Thus, all rows in its adversarial risk table have us as the threat source, and all rows in our table have the adversary as the threat source. If we let risk (to X from Y) denote the risk to X from threat source Y, conceptually we have:

$$\text{CS} = \text{risk (to adversary from US) / risk (to US from adversary).}$$

If $\text{CS} > 1$, then the adversary's risk is higher than ours. That means we are in a better position to affect its systems and operations than conversely; in military terms, it is similar to the notion of having air superiority. If $\text{CS} = 1$, we are equally matched. And if $\text{CS} < 1$, we are at a disadvantage; the adversary can harm us more than we can harm it.

Although CS is expressed as the ratio of two risk scores, the risk methodology outlined earlier does not yield a single estimate for risk but rather a risk estimate for each threat event. Further, these estimates could be qualitative rather than quantitative. To produce a single estimate of risk, the risks for the individual threat events must be combined in some way. If the risk estimates are numeric, this might be done by taking their weighted average,


United States
Adversary
Threat source with capability and intent to conduct cyber ops (threat events)
Threat source with capability and intent to conduct cyber ops (threat events)
Potential cyber attacks
Targets with vulnerabilities & defenses
Impacts to cyber systems & organizations
Targets with vulnerabilities & defenses
Impacts to cyber systems & organizations
Assess adversary risk from United States
United States
Adversary
Threat source with capability and intent to conduct cyber ops (threat events)
Threat source with capability and intent to conduct cyber ops (threat events)
Potential cyber attacks
Targets with vulnerabilities & defenses
Impacts to cyber systems & organizations
Targets with vulnerabilities & defenses
Impacts to cyber systems & organizations
Assess US risk from adversary

(a) Risk to adversary from US cyber threat

(b) Risk to United States from adversary cyber threat

Figure 17.2. Assessing cyber strength from US perspective

Note: Solid lines represent potential cyber attacks; dashed lines represent information flows for risk assessment.

where the weights reflect the priority of the threat events. If the risk estimates are qualitative, they might be converted to numbers and then used to produce a weighted average. Alternatively, if the threat events for each side are equivalent, rather than reducing each side's risk to a single score, risk could be expressed as a vector of scores. With that approach, we can determine the strength of the United States relative to the adversary for different types of cyber attacks.

While the focus here is on cyber operations, the same reasoning applies to other domains. To assess the strength of any type of military force against an adversary, one needs to consider the adversary's risk relative to these forces. In the domains of land and sea, geography especially is an important factor. Army forces, for example, may be capable of defeating almost any enemy on a conventional battleground, but if the conflict takes place in a highly populated urban environment, they may lack the training and experience to fight effectively in that environment. Similarly otherwise strong naval forces might have little to offer against an adversary that is landlocked.

In performing the risk assessments needed to measure cyber strength, we need to consider every cyber system that could be the target of a cyber operation. In addition to military systems, they might include civilian systems such as those used for communications, electric power distribution, or finance. We will say more about this issue later when we discuss scope.

Although methodologies are available for estimating the impacts and losses from cyber attacks (battle damage assessment) and for conducting risk assessment, they have not been combined in the manner proposed here to assess cyber strength in the context of cyber war. In particular, the idea of conducting a risk assessment of adversary systems while using ourselves as the threat source is novel, as is the idea of looking at the adversary's threat in terms of the risk it poses to our systems and not just in terms of its capabilities and intent.

Assessing capabilities and intent, however, is a large part of the picture, and the approach introduced here can build on earlier efforts to do that. A team at the Naval Postgraduate School developed a methodology for assessing the state threat by examining not only a state's military cyber capabilities but also what is going on more broadly inside the state regarding industry, academia, and hackers. In the process, the methodology was used to assess the cyber threats of Iran and North Korea.[3] While the approach was qualitative and ad hoc, a subsequent effort used the Situational Influence Assessment Module (SIAM) influence modeling tool to create a more quantitative approach. The resulting Cyber Warfare Capability Model uses a four-level, hierarchical model to assess a state's cyber capability.[4] In addition to the Naval Postgraduate School's work, a University of New Hampshire research team, under the direction of Andrew Macpherson, developed a Cyber Threat Calculator to assess both the state and non-state cyber threat in terms of capability and intent.[5] Technolytics published numerical scores of cyber capability and intent for more than sixty countries, but it did not describe the methodology used in its assessments.[6]

ISSUES

While conceptually straightforward, the approach outlined in the previous section for assessing cyber war is complex and difficult. This section discusses some of the issues raised. Although many of these problems pertain to assessments of war in general, others are peculiar to or aggravated by cyber war.

DEALING WITH COMPLEXITY AND UNCERTAINTY

Risk assessment is hard, uncertain, and speculative. It is difficult, if not impossible, to identify and assess all of the factors contributing to risk, including threats, vulnerabilities, impacts, and likelihoods. There are too many unknowns and insufficient data to ground assessments. Knowledge is incomplete and the future uncertain. Security researchers are continually finding new vulnerabilities and methods of attack, and cyber attacks can have cascading effects, owing to dependencies.

Consider the task of assessing our risk from adversarial cyber threats. We need to know the adversary's cyber capability, intent, and targeting strategy along with the types of cyber events that could arise during its cyber attacks. We need to know whether our own systems and operations are vulnerable to these attacks and the likelihood of the attacks succeeding. We need to know the impact of successful attacks, not only to cyber systems, but also to operations, organizations, and the nation. We need to know the likelihood of these impacts being realized. None of these factors are easy to determine.

Each year, thousands of new vulnerabilities in software systems are discovered and reported to vendors and the public. According to the security firm Sourcefire, more than five thousand new software vulnerabilities were reported in 2012 alone.[7] This number does not even cover the cases where security is inadequate because of weak passwords or poor security settings. Although tools are available for locating and fixing software vulnerabilities that are already known, these tools are likely to miss vulnerabilities that have not yet been discovered and disclosed. If the adversary finds and develops an exploit for one of these unknown vulnerabilities, its attack is likely to succeed. Such exploits are called zero-day exploits because the time from the disclosure of the vulnerability to the release of the exploit is zero days. Indeed, it may be the use of the exploit in a cyber attack that brings about the disclosure and subsequent remediation of the vulnerability. Such was the case of Stuxnet, which exploited four previously unpublished vulnerabilities. Most cyber attacks do not employ zero-day exploits; instead, they take advantage of vulnerabilities that have been known for months or years and for which fixes are available but not installed. But even organizations that are diligent about security and installing security updates can still be vulnerable to zero-day attacks.

Zero-day exploits are bought and sold in underground and legitimate markets before they are released, sometimes going for hundreds of thousands of dollars. They provide a lucrative source of income for independent researchers who like to hunt for new vulnerabilities and develop exploits for them. Many companies have “bug bounty” programs to encourage researchers to report vulnerabilities to the companies, which want to fix them, rather than to other parties that may exploit them nefariously; but militaries also develop and purchase zero-day exploits for possible cyber warfare operations. Knowing what zero-day exploits the adversary might have or obtain, and how they could affect our own systems, is obviously problematic.

In addition to knowing about possible zero-day attacks, we need to determine the adversary’s other capabilities, including its methods of targeting; penetrating, controlling, and planting backdoors, spyware, and other forms of malicious software (malware) on systems; exfiltrating data; disrupting service; and so forth. We might reasonably assume that the adversary has certain capabilities that are commonly observed in cyber attacks emanating from a variety of threat sources, but we might miss learning about its unique methods that have not yet been observed in actual attacks.

Military operations can depend on many complex and interdependent cyber systems. To fully understand the possible impact of cyber attacks, including their indirect effects on operations and missions, we need to be able to map the dependencies of cyber systems on each other, as well as the dependencies of operations on cyber systems. Doing so for an organization the size of the US military is a daunting task. But without understanding the dependencies and the vulnerabilities they introduce, we may not know that the loss of some logistics or surveillance system, for example, could make deploying troops, executing a particular operation, or achieving mission objectives impossible.

The problem gets even worse when we factor in the civilian systems that the military depends on, including telecommunications and power systems. We will say more about this point later when we discuss scope.

Assessing the risk to the adversary from our cyber attacks is also problematic. While we can reasonably assess ourselves as a threat source to an adversary, we are unlikely to know as much about its systems or its vulnerabilities and dependencies. Consequently, we might think that a proposed cyber attack will succeed, when in fact it will not, or that the attack will cause less collateral damage than it does when executed. Without a complete picture of the adversary's systems and vulnerabilities, we might also miss seeing potential methods of attack. This brings us to the next issue.

SEEING THROUGH THE ADVERSARY'S EYES

In general, it is easier to assess our own strengths and weaknesses than those of another party. Yet to determine where our cyber forces stand relative to those of an adversary, we must be able to evaluate the adversary both as a threat source to us in an assessment of our risk and as a target of our cyber operations in an assessment of its risk. These assessments will only be as good as the data on which they are based, underscoring the need for solid intelligence about the adversary.

Further, to fully appreciate the adversary as a threat source, we need to know not only its capabilities and intents but also how the adversary views us as a target of its operations. If it thinks its cyber operations will succeed (i.e., our risk to its attacks is high), it may be more likely to launch the attacks than if it thinks the attacks will fail to produce the desired effects. This suggests the possibility of presenting our systems in a way that leads the adversary to conclude that the systems are immune to its attacks.

Similarly, it is useful to know how the adversary views us as a threat source. If it thinks we are capable of causing severe harm, it might be less willing to engage us in cyberspace or even in other warfare domains. Conversely, if it thinks its systems are adequately protected from our attacks, it might be more willing to attack ours or less diligent about defending its own.

Battle damage assessment is also more difficult when applied to the adversary than to ourselves. We might not know if certain effects were achieved, especially indirect effects on its operations. We can reduce this potential blindness by integrating a cyber espionage capability into our operations that reports effects, but doing so is unlikely to produce as good a picture as "being there."

CONTROLLING SCOPE

During war valid targets for military operations can include civilian infrastructure such as bridges and electric power systems that serve military objectives when the operations are conducted according to the principles of the law of armed conflict (LOAC). The same would be true of military cyber operations conducted during war. They could potentially target civilian cyber systems, for example, to temporarily disrupt power or telecommunications in a conflict zone. In addition, an adversary might not even abide by LOAC, further broadening the scope of its cyber attacks.

Thus the risk assessments used to determine cyber strength need to take into account risks to potential civilian systems as well as military ones, especially when military systems or operations depend on the civilian systems. For example, if we want to know if the adversary's cyber forces can disrupt or damage our power grid, we need to evaluate the risk those systems operating the grid face from the adversary. Conversely, to determine if our cyber forces can affect the adversary's power systems, we need to assess what risk we pose to its power systems.

However, conducting a risk assessment across our military and our adversary's, or even across segments of two militaries fighting a particular war, is daunting enough without also factoring in risks to civilian systems. As a practical matter, it will be necessary to control the scope of these risk assessments.

One way of controlling scope is to limit the breadth of the assessments—that is, the number of target systems examined. For example, we might only evaluate risks to military systems that are critical to particular operations against the adversary and rely on the general risk assessments performed by the owners of civilian and other military systems as part of their overall cyber security efforts. Although these assessments would not be tailored to a particular adversary during war, they would be better than nothing. Alternatively, we might control scope by limiting the depth, or the level of detail, of the assessments. We could also take a hybrid approach, examining a few critical systems in detail while taking a higher-level approach across a broader set of systems.

RECOGNIZING CYBERSPACE AS A GLOBAL, PERPETUAL CONFLICT ZONE

Cyberspace is constantly under attack by a variety of state and non-state actors, including criminals, spies, protesters, and hackers. It is a perpetual conflict zone, where borders are usually ignored and attacks can be far-reaching and widespread. A single attacker might compromise and control tens of thousands of computers located in dozens of different countries, commanding them to conduct a coordinated, distributed DoS (DDoS) attack against a target across the world. Prolexic, a security firm that specializes in DDoS and network protection, observed more than seven thousand DDoS attacks per day on average in 2013.[8] A single attack can generate tens of gigabits of traffic per second and shut down websites and services.

Of course, systems face more than DDoS attacks. Cyber spies exfiltrate terabytes of data from systems they penetrate, with major operations such as those from China scooping up data from dozens of organizations in multiple countries. Criminals conduct billions of dollars' worth of cyber fraud annually. Protesters such as Anonymous deface or hijack thousands of websites, take over hundreds of Twitter and other accounts, and disclose sensitive personal and organizational information, in addition to being a major source of DDoS attacks. Hardly anyone is immune to cyber attacks, and any device connected to the Internet is likely to be a target, even as it successfully wards off the attacks.

Consequently, when two states (or other political entities) are engaged in warfare, they also have to worry about cyber attacks from actors besides their adversaries. An attack from a third party could impact the state's military capabilities, including, for one, the ability to deploy offensive cyber weapons against the adversary.

This issue could be addressed by including all threat sources in our risk assessments; that is, we could conduct general risk assessments rather than ones tailored to the adversary as a single threat source against us and to our cyber forces as a single threat source against the adversary. However, the result will be more a determination of the relative cyber security posture of us versus the adversary than of the relative cyber strength of us against the adversary. We could get the benefits of both general and tailored risk assessments not only by focusing on ourselves and the adversary as threat sources but also by including other threat sources whose cyber attacks could have serious effects.

DEALING WITH PATRIOTIC HACKERS

In traditional domains of warfare—land, sea, and air—non-state actors tend to leave the fighting to military forces. Indeed, under the international LOAC, they are not supposed to fight except under official state control (e.g., as militias of the state). In cyberspace, however, it is quite common to see patriotic hackers take up cyber arms. During the Russian-Georgian conflict in 2008, for example, pro-Russian hackers conducted many if not most of the attacks in cyberspace. They were recruited on Russian-language web forums such as stopgeorgia.ru and given instructions and tools for attacking Georgian sites. They launched DoS/DDoS attacks, defaced websites, and interrupted Georgia's Internet connections to the rest of the world, seriously impacting Georgia's ability to communicate with its citizens and the international community through cyberspace.[9] More recently, the civil war in Syria has inspired both pro-regime hacking groups, such as the Syrian Electronic Army, and anti-regime groups, such as the Hackers of the Syrian Revolution.[10]

During wartime patriotic hackers effectively add to the cyber forces of the state or non-state entity they support. They increase the entity's threat without introducing any significant risk to it, which is already a legitimate target of the opposition. Even if the patriotic hackers become targets themselves, cyber attacks against them are unlikely to impact the larger entity and its ability to conduct cyber war. In assessing cyber war, therefore, including patriotic hackers as a component of each side's cyber threat seems reasonable. While their capabilities may not be as sophisticated as those of the entity they support, patriotic hackers may be more brazen and nondiscriminatory in their targeting.

DETERMINING ATTRIBUTION

Determining the source of a cyber attack can be difficult. Attackers can hop through intermediary sites, hide their tracks with tools such as The Onion Router, and erase evidence of their attacks. Often what appears to be the source of an attack is just another hacked computer that was compromised and exploited to obscure the identity and location of the attack's true source.

To conduct cyber battle damage assessment against our own systems, we need to know which attacks originated with the adversary and therefore which effects can be attributed to it. Because cyberspace is constantly under attack by many parties and establishing attribution is difficult, it may be hard to distinguish attacks by the adversary from those by others, thus complicating the task of determining damages brought on by the adversary.

Attribution is less of an issue in assessing the effects of our cyber attacks against the adversary. In that case, we know what we did. Even if we observe multiple effects to adversary systems, we might reasonably be able to determine which ones we caused. However, because the main reason for assessing the damages to their systems is to determine whether we are meeting mission and operational objectives, it may matter less whether we produced certain effects as that the effects were achieved.

ABIDING BY THE LAW OF ARMED CONFLICT

For the most part, the preceding discussion assumes that we are already at war, and the question is how to assess the cyber component of that war—namely, the cyber battle damages and the relative strength of our cyber forces against the adversary's. However, another issue arises before the onset of a clearly defined war, and it involves determining the conditions under which a cyber attack could be viewed as an act of force in violation of the LOAC. In particular Article 2(4) of the Charter of the United Nations prohibits states from using force against other states (except for self-defense and under a UN Security Council resolution): "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Although the term "force" is not defined, it is generally understood to include armed attacks from traditional military forces.

Because the UN Charter was written long before cyberspace became a domain of warfare, it does not explicitly address cyber attacks. Nevertheless, a general consensus has emerged that the UN Charter and LOAC more generally apply to cyberspace. Thus, to determine whether a cyber attack violates Article 2(4), we need to know first and foremost whether it constitutes a use of force.While several scholarly works address this issue, the *Tallinn Manual*, which was produced by an international group of experts, is the most thoughtful and thorough treatment of cyber war under LOAC to date.[11] The manual offers nearly a hundred rules for applying LOAC to cyber warfare. Several of the rules pertain directly to Article 2(4), with rules 10, 11, and 12 being especially relevant. Rule 10 prohibits cyber attacks and threats of cyber attacks that constitute force: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful." Rules 11 and 12, respectively, specify the conditions under which a cyber operation constitutes a use of force or threat of force. Rule 11 defines the use of force: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[12] Rule 12 addresses the threat of force: "A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force."[13]

These definitions bring us back to cyber battle damage assessment. To know whether a cyber attack is a use of force, we need to determine first its effects and then whether those effects rise to the level of force in traditional military domains. The *Tallinn Manual* provides guidance for the latter, acknowledging that some cyber operations would not rise to the level of force. The guidance includes criteria first introduced by the manual's editor, Michael Schmitt, that are sometimes referred to as the Schmitt criteria.

Together with other articles of the UN Charter, Article 2(4) falls in the area of LOAC referred to as *jus ad bellum*, or the law of conflict management. LOAC has a second part that is called *jus in bello*, or the law of war. While jus ad bellum is concerned with promoting peace and avoiding hostilities, jus in bello is concerned with fighting ethically and minimizing suffering during war. Jus in bello is often expressed as a set of principles that relate to the distinction of combatants from noncombatants, military necessity, proportionality, indiscriminate weapons, superfluous injury, perfidy, and neutrality. The *Tallinn Manual* also provides guidance in the form of rules for applying the principles of jus in bello to cyber operations. When conducting a battle damage assessment during war, this guidance may be useful for determining whether our cyber operations and those of the adversary are abiding by jus in bello.

Although the *Tallinn Manual* provides helpful guidance for assessing cyber attacks, that guidance is neither definitive nor black and white. Determining whether a particular cyber operation would violate LOAC is still subject to interpretation.

KEEPING UP

Cyberspace is a rapidly evolving domain, with a steady influx of new technologies and applications. One of the challenges in assessing cyber war is simply keeping up with changes in the cyber battlefield—that is, the weapons and systems that may be used or targeted in cyber attacks. New technologies can provide new opportunities for conducting cyber attacks, new vulnerabilities to exploit, and new methods of defense. Even software upgrades for operating systems, networks, and applications can positively or negatively affect risks.

One particularly challenging aspect of this evolving environment is that a cyber weapon can become obsolete after a single use, for releasing the weapon exposes the security flaws that it seeks to exploit and, in turn, can lead those responsible for the flaws to rectify them. No other domain of warfare has such a short life cycle for its weapons. The same type of bomb or missile, for example, can be used again and again, as conventional defenses are much slower to adapt.

Consequently cyber weapons are constantly evolving to get around the latest fixes and updates to the signatures used by antivirus products and intrusion prevention systems. The security firm McAfee, for example, reported seeing 100,000 new malware samples *per day* in 2012.[14] While most of them are variants of existing malware and many pose little threat, the raw numbers reveal the magnitude of the problem of keeping up in this dynamic environment.

CONCLUSIONS

This chapter introduces a framework for assessing cyber war that builds on the elements of risk assessment. The framework can be used to assess both the effects of cyber attacks (battle damage assessment) and the relative cyber strength of our forces against an adversary. Although the focus here has been on cyberspace, the framework might also prove useful for assessing war in other domains where operations are kinetic and their effects physical. It is less clear whether the framework is useful for assessing information and influence operations other than cyber attacks, such as what the Department of Defense once called psychological operations and now calls military information support operations. For those types of operations, it is not clear whether the standard risk variables—namely, threats, vulnerabilities, effects, and likelihoods—even apply.

While perhaps simple and straightforward in principle, risk assessment is complex and difficult in practice. It is highly speculative and fraught with uncertainty. We offer the framework as a way of thinking about cyber war assessment and identifying the variables and issues that need to be considered. Although its application to cyber battle damage assessment seems reasonably straightforward, we leave open whether it could be practically applied to assess cyber strength.

Another limitation of the framework introduced here is that it does not address the dynamics of cyber conflict, including an adversary's responses to cyber attacks and the potential escalatory effects of cyber operations. While important, this topic is left for future study.

NOTES

1. R. J. Kissler, ed., "Glossary of Key Information Security Terms," Revision 2, NISTIR 7298 (Gaithersburg MD: National Institute of Standards and Technology [NIST], May 2013).
2. NIST, *Guide for Conducting Risk Assessments*, Special Publication 800–30 (Gaithersburg MD: National Institute of Standards and Technology, September 2012).
3. Dorothy E. Denning, "Assessing the CNO Threat of Foreign Countries," in *Information Strategy and Warfare*, ed. John Arquilla and Doug Borer (New York: Routledge, 2007), 187–210.
4. Brian D. Cummings and Aric L. McElheny, "Developing a Software Model to Assess a Nation's Capability to Conduct Sustained, Offensive Cyber Warfare" (thesis, Naval Postgraduate School, September 2011), https://www.hsdl.org/?view&did=691268.

5. Lori Wright, "Who Are the Greatest Cyber Attack Threats to the United States?," *University of New Hampshire News*, January 25, 2007, http://www.unh.edu/news/cj_nr/2007/jan/lw25cyber.cfm.
6. Technolytics, *The Cyber Commander's Handbook* (McMurray PA: The Technoly tics Institute, 2009), 12–13.
7. Yves Younan, "25 Years of Vulnerabilities: 1988–2012," Sourcefire Vulnerability Research Team, 2013, https://labs.snort.org/blogfiles/Sourcefire-25-Years-of-Vulnerabilities-Research-Report.pdf.
8. Prolexic, "Knowledge Center," http://www.prolexic.com (accessed November 1, 2013).
9. Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Estonia: Cooperative Cyber Defence Centre of Excellence, 2010), https://ccdcoe.org/publications/books/legalconsiderations.pdf.
10. SalamaTech, Syrian Digital Safety Project, "Flash Note: Syria; Syria's Hacker Wars" (Ontario: The SecDev Foundation, October 8, 2013), http://new.secdev-foundation.org/wp-content/uploads/2014/08/Flash-Note-Syria-13-Syrias-Hacker-wars.pdf.
11. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).
12. Ibid., 45.
13. Ibid., 52.
14. McAfee, "Infographic: The State of Malware 2013," McAfee for Business, April 1, 2013, http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx.