

Cyberwarfare, Law, and Ethics

MANY EXPECTATIONS, ACCEPTED BEHAVIORS AND PRACTICES, and commonly agreed-on laws have arisen over thousands of years of recorded warfare. These laws, treaties, and agreements limited the scope, destruction, and casualties of armed conflict. They allowed nations to lose without being destroyed or to pursue war without making their civilian populations and infrastructure an automatic target. During the twentieth century, those commonly agreed-upon rules of warfare were written into international law in the form of the Hague Conventions and the Geneva Conventions. These international laws, the formation of the United Nations (UN) and its related judicial bodies, and international treaties and agreements provide a useful foundation of laws that can be taken into account in the context of cyberwarfare.

The Geneva Conventions and the additional protocols that have been added to them since their original creation in 1949 have shaped how modern warfare is fought—describing what is acceptable and what is not. They set forth how armed combat is fought, how prisoners of war are treated, and how civilian populations should be treated and protected from indiscriminate attacks. They also set forth how medical aid and other humanitarian efforts should be treated and preserved. The additional protocols added to the Geneva Conventions have recognized changes in warfare, such as new weapons and the increasing role of guerrilla forces. These protocols also address the effects that destroying strategically important facilities, such as nuclear power stations, dams, and the environment itself, can have.

Cyberwarfare tests the boundaries of existing international laws for many reasons. By its nature, it typically requires the use of civilian infrastructure to conduct attacks. The systems from which attacks are conducted are often civilian systems—or the attacks pass through civilian systems as part of their path to government and military targets. In addition, carefully aiming cyberattacks

to target only traditionally acceptable targets can be difficult. Those systems can be hard to distinguish from civilian systems or may actually coexist with them on the same hardware in cloud computing data centers.

Cyberwarfare also creates the potential for unrestricted attacks by nontraditional combatants. It places what may be a possibly far more powerful weapon in their hands in the form of malware. Modern advanced malware is designed to disrupt or destroy infrastructure and computer-based systems and networks. It provides a powerful asymmetric weapon in the hands of insurrectionists and guerrillas as well as the militaries and intelligence operatives of nation-states. In traditional warfare, attacks required significant resources and capabilities to strike at physical structures and personnel. Today, however, attacks can be conducted at the push of a button with an army of silent malware-based zombie systems.

This complex environment makes the interpretation of the existing framework of international law challenging. Fortunately, experts in cyberwarfare attack and defense as well as legal experts have provided an analysis for the United Nations in the form of the Tallinn Manual. The manual examines the existing bodies of law and legal precedent. It couches cyberwarfare in those terms, providing a meaningful way of looking at where cyberwarfare and traditional warfare have strong parallels, and where cyberwar creates real questions.

In addition to legal analysis and responsibilities under international law, the ethics of cyberwarfare are also an important part of the equation for combatants and noncombatants alike. Ethical standards exist for information security professionals, but distinct codes of ethics for cyberwarriors have not been created. Thus, this chapter examines the ethical codes of security professionals to better understand which important elements may be part of the ethics of cyberwar.

Chapter 3 Topics

This chapter covers the following topics and concepts:

- What kinetic warfare is
- What the role of law in cyberwarfare is
- What the ethics of cyberwar are

Chapter 3 Goals

When you complete this chapter, you will be able to:

- Explain critical concepts in international warfare law in relation to cyberwar
- Explain the current state of cyberwarfare law
- Relate existing international law and cyberwarfare activities
- Identify gaps and issues in the application of the traditional law of war and cyberwar
- Explain the role of ethics in computer network defense and attack

Kinetic Warfare

Traditional military conflict has been fought using weapons like bombs, tanks, and guns. Warfare between nations has involved military forces that invaded enemy territory or that fought the opposing country's army, navy, or other forces. At times, civilians were involved either because they were caught in the combat area, due to their role in a militia or resistance, or because warfare had grown to involve every possible target.

As new forms of warfare have evolved that do not require the same type of direct, visible force, a new terminology has arisen. It describes the traditional type of military conflict as **kinetic warfare**. High-technology cyberwarfare is called **nonkinetic warfare**.

The international body of laws for military conflict between nations provides a useful starting point when examining cyberwarfare in a legal context. Although cyberwar provides new capabilities and raises new questions, many of the definitions used in kinetic warfare match those that exist when cyberattacks cross into the physical world.

International Law and Kinetic Warfare

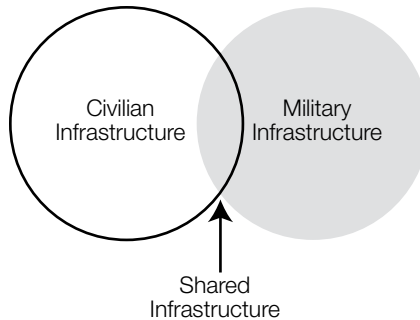
Laws of warfare have existed in one form or another since ancient times. But treaties and international agreements in the twentieth century have created widely accepted standards for the conduct of war. The first major international agreement on warfare was the 1899 Hague Conventions, which defined rules and customs of war on land, set limits on certain types of weapons, and banned poison-gas projectiles. In 1907, the Hague Conventions added rules on how to start hostilities, naval warfare, and updates to the previous customs and laws of land warfare.

NOTE

Earlier international laws existed, including earlier Geneva Conventions. However, they did not have the same breadth and widespread adoption as the Hague Conventions and the later Geneva Conventions.

FIGURE 3-1

Civilian, military, and shared use of infrastructure.



Over time, the need for updates and a newer body of international law on warfare became obvious, and in 1949 the Geneva Conventions were signed. In 1977, additional protocols were added, clarifying and adding additional rules to the originals. Since 1977, the Geneva Conventions include rules on the treatment of prisoners of war; how medical personnel, journalists, children, and civilians should be treated; and a wide variety of other rules of warfare. They have been updated to deal with new technologies, including nuclear reactors, poisonous gases, and other new types of warfare and weapons. They define when **civilian infrastructure** is protected and when military use of infrastructure results in civilian infrastructure becoming a valid target (see Figure 3-1).

In addition to the Geneva Conventions, the United Nations Charter and foundational documents provide additional rules for member countries, particularly around the use of force and declaration of war between member countries. The United Nations also provides international courts, which have examined conflicts between member nations and have released rulings about appropriate behaviors and acceptable responses.

The laws of warfare are commonly split into two categories:

- **Jus ad bellum**, Latin for “the right to war.” *Jus ad bellum* law determines when nations are allowed to enter into war. International law now typically allows nations to respond to immediate threats, or active attacks, but not simply to declare war. The UN Charter requires nations to receive UN approval before using force against another nation except in self-defense. The same rules require that responses to attacks be proportionate to the attacks, and that they should not have overly broad effects.

FYI

The laws of warfare are based on consensus. In other words, they exist only because countries agree to them and agree that they are appropriate. The way that each country interprets the laws of war can vary, and often changes over time as circumstances, leadership, and public feelings change. In addition to the varying interpretations of the rules of war, some countries have agreed only to portions of existing treaties or choose to not sign them at all. Thus, although the laws of war are well known, they are not consistently followed, and they are constantly being challenged.

- **Jus in bello**, Latin for “the law of war.” *Jus in bello* law determines what is allowable during wartime. The Geneva Conventions define acceptable conduct during war such as that previously mentioned, and thus are *jus in bello*, rather than the UN charter’s *jus ad bellum* law.

Like most laws and standards, changes in how warfare is fought can lead to changes in the laws and standards. Cyberwarfare changes how attacks are conducted and can blur the lines between civilian and military systems and infrastructure. Further, the existing laws of armed conflict don’t fully cover cyberwar. Even when cyberwarfare and kinetic warfare intersect, the way existing standards apply can appear uncertain.

Legal Review and Legality of Actions

Legal authority to determine what is and is not legal according to international law primarily resides with international courts like the International Court of Justice (ICJ), the primary judicial branch of the United Nations. The ICJ has typically followed the philosophy that “that which is not prohibited is permitted” in its findings on international law and warfare.

Of course, the findings of the court are only binding on those countries that agree to them. This means that at times countries may not agree to be bound by the court’s rulings, and states that are not members of the United Nations are sometimes not subject to the UN’s influence.

Cyberwarfare Law

Countries throughout the world have written laws regarding cyberattacks that address their own internal needs. However, the international laws of warfare in the form of the Geneva Conventions and UN decisions have not been updated to address cyberwar techniques and technologies. Major cyberattacks, such as Stuxnet, Aurora, and Flame, as well as the increasing development of cyberwarfare capabilities by nation-state militaries, demonstrate that this is an area that nation-states intend to use more heavily in the future.

Due to the lack of precedent from international courts, and the quickly evolving capabilities of cyberattackers, effective law covering cyberwarfare may be difficult to create. Until the Geneva Conventions are updated, and the UN creates rules around cyberwarfare activities, the existing commonly accepted rules of warfare will be applied where they fit. Nation-states will exploit the gaps between what was possible in kinetic warfare and the new capabilities that cyberwarfare makes available to them.

Cyberwarfare in a Kinetic Warfare Context

The Stuxnet attack offers a look at the growing role of cyberwarfare as an alternative to kinetic warfare. The strike, which was aimed at Iran’s uranium enrichment facilities, used a variety of network attack techniques to penetrate non-network-accessible infrastructure. Prior to the advent of techniques like those used in the Stuxnet attack, the only

ways that a nation could have disabled an enrichment facility would have been through a kinetic attack—through military action, or via intelligence operatives or moles planted in the facility taking action and thus risking their lives.

Cyberattack methods also have the potential to disable, disrupt, or even redirect military computers and computer-controlled systems. The increasing use of drone-based weapons systems and computer-controlled platforms, including ships, missile systems, and other major weapons platforms, means that a computer network attack could result in the ability to take over kinetic warfare systems.

Cyberattacks that result in kinetic attacks might also result in escalation between combatants that did not actually intend to be at war. A hijacked drone or missile system that strikes the cyberattacker's target rather than that of the country that owns the weapons system would trigger the target country's right to self-defense against the apparent aggressor. Setting a nation-state up to wrongly bear the blame for an attack is not a new concept, but doing it remotely using the innocent state's own weapons systems and networks has the potential to change international relations quickly.

Kinetic Warfare Law in a Cyber Context

Kinetic warfare can also cross over into cyberwar when the combatants respond to or preempt cyberattacks using traditional means of warfare. A defender may be able to stop an attack in the following circumstances:

- If the location that the attacks are coming from can be determined
- If the network carrying the attacks can be targeted
- If the individuals who are conducting the attack can be captured or killed

The ability to respond kinetically to stop a cyberattack can be challenging. Many of the large-scale cyberattacks up to this point have been hard to track. And some, such as the Stuxnet, Aurora, and Flame attacks, have been very difficult to attribute to specific attackers or physical facilities. In those cases, physical attacks would likely have been overly broad because the individuals and computing resources used to create and launch the attack were not known.

This doesn't mean that kinetic attacks aren't possible in cyberwar. As computer network attack and defense capabilities continue to receive significant investment by military forces in many countries, the likelihood of combining kinetic strikes and cyberwarfare capabilities will increase. Over time, strikes that combine a cyberattack intended to disable systems or to soften defenses prior to a kinetic strike or invasion are far more likely. Countries that lack strong computer network defense and attack capabilities are likely to respond with traditional military capabilities.

With the intersection of the commonly accepted international rules of warfare and cyberwarfare remaining undefined in many areas, the need for a better understanding of where existing laws and traditional rules are useful and where they aren't is increasingly obvious. Various legal experts have worked to develop mappings between the large number of existing laws and treaties, as well as common wartime customs and what is possible during cyberwar. One of the best examples of this type of work is the Tallinn Manual.

The Tallinn Manual

The **Tallinn Manual** is an in-depth review and analysis that provides nonbinding advice based on the existing international body of law around armed conflict and related topics. It was created for the NATO Cooperative Cyber Defence Centre of Excellence, an organization sponsored by the United States, Italy, Spain, Germany, and a number of other nations.

The Tallinn Manual is a response to a growing focus on cyberattacks by both nation-states and nonstate actors, and the challenges those attacks provide when nation-states attempt to determine if their activities or those of their attackers are covered by international law. International views on whether the existing laws and treaties regarding warfare apply to cyberattacks and cyberwarfare vary, and the threshold conditions that determine when a state of war exists are often a point of contention.

The Tallinn Manual points out that the International Court of Justice has stated that existing law regarding armed conflict applies when “any use of force, regardless of weapons employed” occurs. At the other end of the spectrum from the International Court of Justice’s take on the use of force, the court’s predecessor, the Permanent Court of International Justice of the League of Nations, stated that “acts not forbidden in international law are generally permitted.” Because most of the existing international laws of warfare were written before cyberwarfare techniques and capabilities were even imagined, many of the tactics, technologies, and potential impacts of cyberattacks and defense are not accounted for directly in international law.

Much like the differences in views on international warfare laws that exist for traditional kinetic warfare, individual nations have differing views on what is acceptable during cyberwar. The United States, for example, states in its International Strategy for Cyberspace that “development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.” It also notes that the right to self-defense is a critical part of existing law and the United Nations Charter.

Despite varying opinions on how existing laws and treaties should be applied to cyberwarfare, the Tallinn Manual provides a useful framework to understand, interpret, and analyze international law in a cyberwarfare context. The following sections review major parts of the Tallinn Manual and its analysis of existing laws and norms when applied to cyberwarfare, combatants, civilians, nation-states, and the use of force in cyberwar.

NOTE

As this chapter describes important parts of the Tallinn Manual, the text often refers to it as “the manual.”

NOTE

The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) was created to improve cooperative cyberdefense capabilities for its member nations. It conducts cyberdefense research, runs cyberdefense (CND) exercises in a game style, provides courses on defense and technical subjects, and conducts conferences on cyberconflict.

FYI

Critics of the Tallinn Manual have pointed out that the manual doesn't clarify a number of topics, including what a cyberweapon is and how to ensure that targets for counterattacks are truly allowed targets. In addition, Russian critics have been vocal about what they claim are U.S.- and NATO-centric views taken by the experts who wrote the manual.

Sovereignty, Jurisdiction, and Control

One of the first things that must be settled during warfare is the question of where nations have authority, where they can extend that authority, and when they are expected to be in control of actions that they, or others, take on their behalf. These questions are determined by the nations' sovereignty, their jurisdiction, and their control. The Tallinn Manual examines each of these concepts in the context of cyberwar, where each question is made more complex due to the Internet's international reach. In fact, national borders are far less concrete when applied to computer networks and electronic communication systems.

Sovereignty

Sovereignty, or the right to exercise the functions of a state independently, is a key part of law when applied to cyberoperations and infrastructure. Cyberinfrastructure in a nation's territory is thus subject to that state's control, and the infrastructure is protected by the state's sovereignty, regardless of whether it is state or privately owned. That also means that nation-states can control their cyberinfrastructure, including access to the Internet, traffic sent over telecommunications networks, and other computer networks.

National sovereignty is also the foundation of international law that prohibits other nation-states from taking action against the territory or citizens of another sovereign nation. One important part of cyberwarfare law that has not been explored in international law is the effect of nonstate actors in cyberwarfare as a violation of sovereignty.

Jurisdiction

A nation-state's **jurisdiction** is the authority to enforce its will in criminal, civil, and administrative procedures within its territory and outside of its territory where allowed by international law. Cyberwarfare jurisdiction can be especially difficult due to the Internet's international nature and the fact that systems and networks belonging to groups who fall under a nation-state's jurisdiction may not be physically located in that country. Thus, jurisdiction can be difficult to determine during a cyberattack, and the location of a country's sovereign territory in the electronic world can be hard to distinguish.

Mobile and wireless technologies can make jurisdiction difficult to determine as well. The Tallinn Manual's examination of jurisdiction notes that nation-states can claim jurisdiction if individuals operated inside of their territory. Unfortunately, proving that an individual was within a nation's territory when he or she conducted an attack may be difficult to prove.

The manual describes two forms of commonly recognized jurisdiction:

- Subjective territorial jurisdiction, which allows a nation-state to apply its laws if an activity is started within its territory but completed elsewhere—even if it has no effect within the state
- Objective territorial jurisdiction, which provides nation-states jurisdiction over individuals who act against or upon the state, even if their activities were conducted outside of the state's territory

These two forms of jurisdiction provide the opportunity for states to take action against cyberattackers who violate national law from outside of the nation's borders, as well as those who attack other nation-states from within their borders. This means that multiple nations may have jurisdiction in some cases, such as when an attack is conducted within one nation's borders against another nation via the Internet.

The Cloud's Problem with Jurisdiction and Control

Cloud computing, which uses shared resources at data centers often spread around the world, creates a host of potential problems for questions related to jurisdiction and control. Although the physical servers used in cloud computing are easy to locate, the individuals in control of a given virtual system that exists in a cloud computing environment can be very difficult to identify if they want to remain anonymous. Thus, an attack from thousands of virtual systems located in data centers in a dozen countries around the world is entirely possible. If that occurs, determining which country is responsible for purposes of an appropriate kinetic or electronic response becomes nearly impossible.

The same massive infrastructure that can be quickly repurposed makes cloud computing useful to both attackers and legitimate businesses and government organizations. The massive number of systems available from cloud providers makes them ideal for attackers who can move their attack systems after each use. They can also use the enormous pools of cloud systems to hide next to civilian systems. In some cases, the same data center and cloud servers running outsourced government services could be used by the attackers who are targeting them.

Control

Under existing international law, nation-states are expected to prevent attacks against other countries from resources and individuals that are under their **control** or located within their borders. In cyberwarfare, this expectation can be extended to systems and networks that exist within their boundaries or which they operate themselves. In fact, a nation-state is expected to exercise control over behaviors like this whether the acts are intentionally committed on its behalf or they are committed by organizations or individuals whose actions can't be directly proven to be on that nation-state's behalf.

The concept of control is necessary to support the sovereignty of other states. States are required to have control to ensure that they respect the sovereign rights of other nation-states. In cyberwar, this is difficult, as cyberattacks can be difficult to detect and can occur very quickly. The Tallinn Manual points out that stopping such attacks can

NOTE

Control is one of the most difficult concepts to transfer from existing international law into cyberwarfare. Although preventing physical attacks isn't necessarily an easy task, it is typically simpler than preventing cyberattacks, which can have massive impact from the actions of just a few systems, and which can be very difficult to detect.

cause harm to the originating state because of the actions required to stop an unknown, large-scale cyberattack. Preventing large-scale cyberattacks might require a country to entirely disable its Internet connection to the rest of the world, or to take major systems offline due to the size of the attack or lack of knowledge of how it works.

Under international law, nation-states that fail to exercise control can be met with proportional force in return. This means that a country that is experiencing an attack, or is about to experience an attack, can strike back in kind. In cyberwarfare, determining that an attack is about to happen and responding in kind is very difficult. Furthermore, determining what type of response is appropriate can be very challenging.

Responsibility

Under international law, nation-states are responsible for actions when they meet two requirements:

NOTE

Responsibility is largely defined by the International Law Commission's Articles on State Responsibility, which can be found at http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf.

- The action can be attributed to the nation-state under international law.
- The action is a breach of international law.

International law governs both action and inaction, meaning that states that neglect their responsibilities under international law can still bear responsibility for that lack of action. The same definitions of international responsibility apply to wrongful acts that do not reach the level of cyberwarfare, but which are against other international laws.

Responsibility is automatically attributed to a nation-state if the actions (or lack of action) are performed by a formally recognized part, or **organ**, of that nation-state, regardless of where it occurs. International law doesn't try to distinguish actions that a state intends to conduct, or which its organs conduct without instruction. As long as the organ is acting in what appears to be an official capacity, the state bears responsibility for its actions. States may also have responsibility assigned to them in some circumstances if they support nonstate actors after the fact, resulting in actions previously taken by those actors being assigned to the state based on international law.

Proving responsibility can be a challenge. In cyberwar, countries can bring to bear three types of proof:

- Forensic or factual proof with information that they can bring to the ICJ or other international bodies demonstrating that the action was taken
- Technical proof, such as log files, network traffic captures, or other similar information that provides documentation of the action
- Political proof, often in the form of communications or claims by the country that is believed to have taken the action

Proving responsibility in cyberwar will remain a challenge. Determining who was in control of a system when it attacked, or if a system in another country was under the control of that nation, can be difficult if the aggressor wants to cover up his or her actions.

The existing body of laws on international warfare has a useful definition for nonstate actors who are provided with rewards for their participation in warfare. Those individuals and organizations are known as **mercenaries**, and they are carefully defined in existing law.

Nonstate Actors and Responsibility

The actions of nonstate actors can sometimes be attributed to nation-states if those actors are acting on the instructions of the state. The Tallinn Manual notes that Article 8 of the Articles on State Responsibility directly cover this situation, stating "the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."

The ICJ has previously decided that states bear responsibility for nonstate actors when they have "effective control" over those actors. The manual notes that effective control typically requires that the nation-state provide instruction, direction, or control, and not just financing or technical knowledge or capabilities. This doesn't mean that providing tools may not be a violation of international law. It just means that the state itself doesn't bear formal responsibility for the action taken by the nonstate actors.

Mercenaries

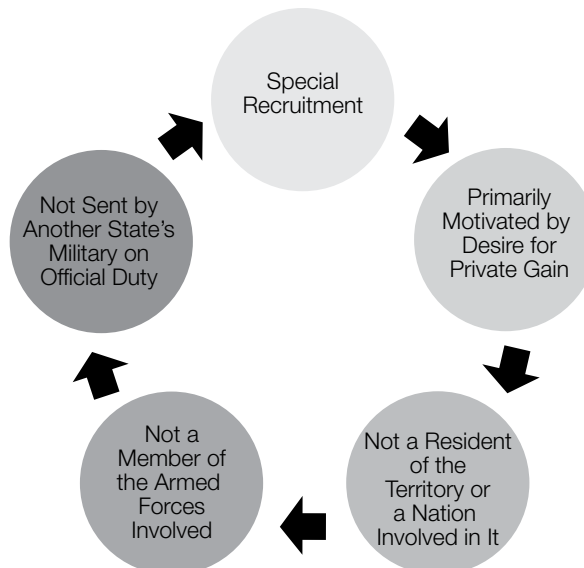
The use of mercenaries, or hired combatants in cyberwarfare, also suffers from the same problems that other nonstate actors do. International law is clear on the definition of mercenaries, as the 1977 addition to Protocol I of the Geneva Conventions lists six key elements in defining if an individual is a mercenary during warfare. By international law, a mercenary is a person who:

- Is recruited locally or abroad to fight in an armed conflict
- Takes part in the conflict
- Is motivated by his or her desire for private gain, which is promised to him or her by a party to the conflict, and that material gain is substantially greater than what is paid or promised to combatants in the armed forces of the party
- Is not a national of the party and does not reside in territory over or in which the conflict is fought
- Is not a member of the forces of a party to the conflict
- Was not sent by a state that is not a party to the conflicts as part of his or her duty in that party's armed forces

Figure 3-2 shows a review process for determining if a combatant is a mercenary based on the Geneva Conventions' definition. Cyberwar's often indistinct boundaries and the potential to be fought across national boundaries mean that identifying mercenaries may be more difficult if individuals or organizations that are not part of a nation-state are employed as part of a nation's computer network attack offensives.

FIGURE 3-2

Identification of mercenary actors in warfare based on international law.



Mercenaries could also be used for computer network defense activities, but this is far less likely to become a matter of international legal importance because computer network defense does not involve the use of force. The use of force and how it can be measured are the next important concepts in cyberwarfare law.

The Use of Force

The use of force is one of the most important points in international law on warfare. Measures of when force is in use, what makes an event a use of force, and what the meaning of a use of force is on an international level are all key elements of existing law.

Under existing international law, the concept of an armed attack is the typical measure of when a nation-state can use force in self-defense. Thus, the experts who wrote the manual believe that cyberattacks rising to the same level of impact as an armed attack would qualify as a use of force. Cyberoperations are much more difficult to measure than a direct armed response, so a means of measuring cyberoperations as a use of force is needed.

NOTE

The Tallinn Manual points to a ruling by the International Court of Justice, which states that “any use of force, regardless of the weapons used” is prohibited based on Article 2(4) of the United Nations Charter. The manual therefore presumes that it is reasonable to apply existing international laws and standards on the use of force to cyberwar.

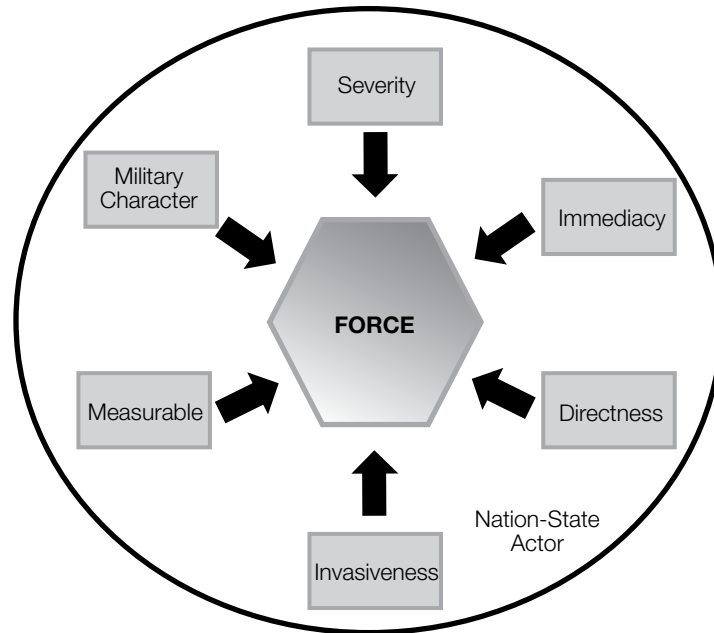
Measuring Force

The Tallinn Manual notes that determining if force was used is a complex process requiring that the actor be a nation-state. The manual suggests six major criteria for measuring whether force has been used:

- The *severity* of the attack or action. Severity is the most important measure, particularly if the actions taken kill or injure people, or destroy or damage objects or facilities. Even if they do not, if the actions have significant scope, duration, or intensity and impact national interests, the manual suggests that the severity may still rise to a level where they are considered a use of force.
- The *immediacy* of the action’s results. Thus, if the actions will impact a nation-state quickly, it will be a more significant issue than a long-term consequence.
- The *directness* of the action’s impact. If an action does not have a direct impact, and instead the action’s results will be felt at a later date—or cannot be immediately and directly linked to the action—the action is less likely to be identified as a use of force.
- The *invasiveness* of the attack or action as measured against the system’s security and how deeply the attack penetrates layers of security. The manual distinguishes between successful intrusions into highly secure environments and compromises of common civilian systems with typical commercial security systems in place.
- The presence of *measurable* damage, either in terms of data destroyed or taken, or systems taken offline, or some other measure. If an action’s results are not easily measurable, it is much harder to claim that force was used.

FIGURE 3-3

Determination of the use of force by a nation-state in warfare.



- The presence of a *military character*. If the attack has a military character, it is more likely to be seen as a use of force. In fact, existing international law specifically mentions military action, making the involvement of a military group or organization more likely to result in the action being considered a use of force.

NOTE

Remember that simply because an action is not immediately attributable to a nation-state does not mean that it cannot eventually be attributed to that state. If a nonstate actor is found to have been operating at the direction of, and with the support of, a nation-state at a later date, or the nation-state takes responsibility for that nonstate actor, the previous attacks could be considered a use of force on behalf of the nation-state.

Figure 3-3 shows how these individual elements map to a determination of the use of force. Remember that the relationship of all of the elements is important to the determination of the use of force, and that the determination is not a simple mathematical calculation. Determination of force by a victim during an attack will be based on what the victim knows. Responses are likely to be based on what the victim thinks an appropriate response might be.

Use of force in cyberwar isn't restricted to government or military organizations. Civilian contractors, mercenaries, and even individuals and groups could reach the threshold for the use of force. Parts of international law don't directly apply to those groups if their actions are not attributable to a nation-state. Although their actions may be against the law, if they are not attributable, they likely fall outside of the international prohibitions against the use of force by nation-states themselves.

Threats of Force

In addition to the actual direct use of force, the threat of the use of force is important to international law. Nation-states can use the threat of force to influence other countries, endangering their sovereignty. Due to this, the UN Charter specifically mentions threats in Article 2(4), “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.”

Cyberwarfare makes threats of force more complex in some circumstances. The ability of nation-states with significant control of the Internet and its underlying infrastructure to damage the commercial and governmental operations of other countries means that the measures of the use of force may shift significantly as international standards are created.

Self-Defense

The right to self-defense is a critical part of international law. The concept of sovereignty and the right of a nation to control and defend its territory lie at the very heart of the laws and accepted customs defining how nations interact. Self-defense in kinetic warfare is often a comparatively simple concept, with aggressors engaging in kinetic attacks

9/11 and the Right of Self-Defense Against Nonstate Actors

The terrorist attacks against the United States on September 11, 2001, resulted in a significant shift in how attacks by nonstate actors were perceived in the context of self-defense by nation-states. In traditional international law, an attack by nonstate actors would not have been considered an armed attack that would allow a country to claim the right to self-defense.

The international community largely supported the U.S. claim to the right of self-defense and generally supported U.S. actions taken in response to the attacks, including widespread military action against al-Qaeda, a nonstate actor. The Tallinn Manual’s panel of experts believes that this extension of the right of self-defense set a precedent that could be used in cyberwar. If nonstate actors conducted a sufficiently damaging attack, the manual’s panel holds that it would be within the rights of the attacked country to respond using force based on the existing rules around the use of force when immediately threatened or under attack.

This becomes more difficult when the use of force in a response violates the sovereignty of another nation that may not be aware of or support the actions taken by the nonstate actors. The use of proportional force may impact the civilian population, and could violate the sovereignty of the nation-state or states in which the attackers are operating, resulting in an escalation of force.

against a defender. The laws of *jus in bello* focus on proportionality of responses, requiring defenders to respond in kind, rather than with excessive force or against a broader range of targets.

In recent decades, guerrilla warfare and combat against insurrectionists have made identifying the attacker in kinetic warfare more complex. Although international law previously recognized only nation-states as potential attackers against whom countries could invoke the right to self-defense, al-Qaeda's 9/11 attack against the United States resulted in much of the international community changing its position on this question.

The manual notes that the right to self-defense against cyberattacks is a reasonable expectation based on both existing law and the international community's reaction to the 9/11 attacks. The more challenging part of exercising the right to self-defense in many scenarios will be identifying the attacker and responding in a proportional way.

International Governmental Organizations

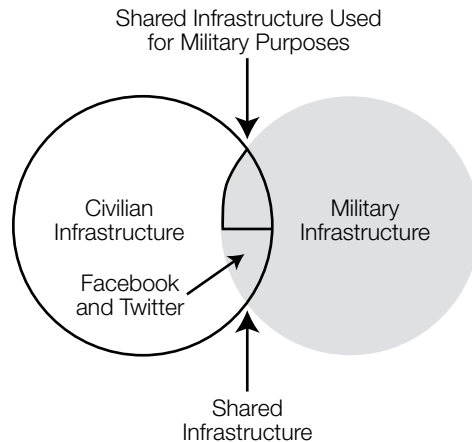
In addition to individual sovereign countries' right to self-defense, the United Nations bears broad responsibility under its charter when determining if acts by nations are one of three types of aggressive acts:

- A threat to the peace
- A breach of the peace
- An act of aggression

The UN Security Council is tasked with determining what type of act occurred or is occurring, can then authorize nonforceful measures, and can escalate those measures to forceful measures if the nonforceful measures fail. The United Nations also takes into account the behaviors of the aggressors, including whom or what they are targeting, such as civilians, infrastructure, or the natural environment.

Civilians and Infrastructure

The Geneva Conventions specifically call out civilians and civilian infrastructure as protected from direct attack. In fact, the Geneva Conventions declare this in a number of areas, including Article 54 of the Additional Protocol I, which prohibits attacks against the objects "indispensable to the survival of the population." Although this has traditionally meant the food supply, it also includes the infrastructure that supports the food supply. As technology has become more important to food production, the Tallinn Manual points out that although the Internet is not necessary to survival, the cyberinfrastructure that supports survival, such as water supply and electricity generation, likely fits into this category.

**FIGURE 3-4**

Facebook and Twitter, civilian, military, and shared use of infrastructure in the cyberworld.

Civilians and Military Use of the Internet

This chapter previously discussed the crossover between military and civilian use of the same infrastructure. In wartime, this has often meant the use of the same communication systems, roads, bridges, and other physical infrastructure. Now, shared use of network and Internet resources is also a concern. Further, the line between what is a military use of infrastructure and what is use of the infrastructure by the military for nonmilitary purposes becomes more important. In Figure 3-4, note the use of shared network infrastructure for military purposes, such as communication and cyberattacks, and the line between that use and the use of other systems by the military, but not for military purposes.

An excellent example of this would be use by military personnel of Facebook or Twitter. In fact, many uses of Facebook and Twitter by military units themselves would likely fall outside the accepted rules on the use of civilian infrastructure for military purposes. Although this fine line has not been decided by an international court, attacking Facebook simply because military personnel or units had a Facebook profile or page does not fit the definition, according to the experts who created the Tallinn Manual.

Prohibited Targets: Children, Journalists, Medical and Religious Personnel, and Nature

The Geneva Conventions define a number of prohibited targets that are protected as long as they are not taking part in hostilities. Here's a list of prohibitions:

- Children are protected under the Geneva Conventions and are prohibited from involvement in armed conflict. Numerous cases in which children have been involved in cyberattacks demonstrate that this may be a particularly difficult protection for nation-states to apply, much as preventing children from fighting in warfare has presented challenges throughout the twentieth and twenty-first centuries.

FYI

The manual notes that “the majority of the International Group of Experts took the position that broadcasts used to incite war crimes, genocide, or crimes against humanity render a journalist a direct participant and make the equipment used [for] military objectives liable to attack, including by cyber means.” As with many of the other impacts of international law on cyberwar, the role of journalists and others in cyberwar may be difficult to determine on a consistent basis and will depend on circumstances and actions at the time.

- Journalists who are engaged in professional missions in armed conflicts are considered civilians, and must be protected as such.
- Medical and religious personnel and material are protected as noncombatants unless they participate in harmful actions. They are to be allowed to perform their duties without interference or harm. The manual interprets this to include medical computer networks and systems, which can be difficult to differentiate in cyberwar. It points out that the rules allowing medical personnel to be armed for self-defense should be interpreted to allow them to have tools that might be useful for cyberwar in their possession without making them a target.
- The natural environment is classified as a civilian object and the Geneva Conventions specifically prohibit attacks that may cause long-term, widespread, severe damage to the environment.

The manual notes that the rules protecting some noncombatants do not mean that their computer systems and networks must be protected beyond the rules that cover civilian infrastructure and systems. Thus, a journalist’s activities and equipment are not provided special protection. In contrast, medical personnel are likely to be protected from such attacks if the attacks would prevent them from performing their duties.

The Conduct of Attacks and Indiscriminate Means

A key element of international law is the prohibition of indiscriminate means of attack. According to the Tallinn Manual, indiscriminate means are those that are not “(a) directed at a specific military objective, or (b) limited in their effects as required by the law of armed conflict.” In addition to the prohibitions of attacks on civilians, weapons and strategies that target broad populations without concern for who will be harmed are banned. Indiscriminate attacks that successfully target legitimate military objectives are still prohibited, because they are not aimed at a specific target. In addition, the manual notes that both military and civilian commanders, as well as their subordinates who carry out their orders, bear responsibility for indiscriminate attacks and ordering indiscriminate attacks would likely be considered a war crime.

The manual also examines the way in which attacks are conducted as well as the means that are used. The experts on the panel specifically note that based on accepted law and precedent, attacks must not do excessive damage to civilians or civilian objects compared with the military advantage they create. In other words, attacks can't do significant damage to civilians in order to gain a minor military advantage. This is particularly important in cyberwar activities, as the shared infrastructure of civilian networks and systems may be an inadvertent target in the path of an attack against military systems.

Espionage, Treachery, and Ruses

Espionage and treachery exist outside of most of the commonly accepted laws of international warfare. The manual notes that the exception to that rule occurs when the action will cause harm or death, thereby meeting the criteria. The manual focuses on the need for the action to be directly linked to the cause of death, and not through a series of unforeseen actions.

Cyberwar creates the potential to engage in **treachery**—acts that lead an adversary to believe that he is entitled to, or obliged to give, protection under the laws of war, while intending to betray that confidence. Falsely identifying computer systems as protected systems, such as those used for medical personnel, or pretending to be civilian systems or infrastructure to avoid attack would constitute treachery. Although pretending to be medical personnel or another protected class of noncombatant is forbidden under the customary rules of war, cyberwar conditions may make separating legitimate protected objects from those falsely appearing to be protected very difficult.

Unlike treachery, a **ruse** is considered a legitimate part of war. A ruse is intended to mislead an enemy without violating the laws of war. Many ruses used in computer network attacks and defenses would fit into this category, such as:

- Creating fake networks and systems
- Providing false information via computer systems
- Launching fake cyberattacks
- Conducting psychological operations
- Redirecting traffic through systems to gain access to the traffic

In essence, the same ruses and deceptions that would be considered a legitimate part of kinetic warfare can be extended to cyberwarfare.

Neutrality

Neutrality is an important concept in kinetic warfare, and is perhaps even more important in cyberwar, as many countries in the cyberattack's path will be neutral. Under the customary rules of warfare, neutral states are protected and can continue to conduct their normal activities without interference from combatants.

NOTE

International law does not directly address espionage acts, meaning that international law does not apply in cases of espionage activity that do not directly violate specific international regulations.

In cyberwar, this means that neutral states must prevent combatants from using infrastructure that is under neutrals' sovereign control. In kinetic warfare, this is easier to do, as national borders can be closed to combatants, whereas closing networks to traffic from warring countries can be difficult if not impossible. If combatants discover that neutral states are allowing the combatants' opponents to use the neutrals' resources, combatants can take action against the neutrals.

The Internet's highly interconnected nature makes the concept of neutrality in cyberwarfare more challenging. This remains one of the areas where international law will require further clarification to provide appropriate protections for neutral countries.

Ethics and Cyberwarfare


Individuals engaged in computer network defense and computer network attacks bring their own ethical standards and those of their profession, military branch, or organization. Although broadly accepted ethical standards specific to cyberwar haven't been developed, there are common ethical standards in existing international law. The critical elements of the laws of war are:

- Self-defense, which prohibits nation-states from indiscriminately engaging in war with other nation-states. Cyberwar's blurred boundaries mean that the concept of self-defense can be a challenging one to define, and thus ethical boundaries for what is acceptable to a nation or organization are important.
- Proportionality, which prevents an escalation of warfare when combat does occur. Proportionality can help to ensure that attacks do not increase in scope. A proportional response is ethically important to help make sure that attacks are not used as an excuse to deploy crippling tools that violate the limitations on acceptable targets and other rules of warfare.
- Limitations on targets, which are important and particularly relevant to cyberwarfare activities due to the shared nature of most major network connections and many computing environments. As the world becomes increasingly more networked, everything from food production to environmental controls and medical systems are all potentially in the line of fire when attackers are focused on government or military systems.

In addition to the ethical concepts that existing and historical laws of war provide, individual practitioners are often trained by information security training organizations that provide their own ethical systems. Professional organizations like those that provide major information security certifications provide codes of ethics that share common concepts, such as:

- Appropriate use of skills and capabilities
- Professionalism
- Adherence to existing laws and standards
- Respect for privacy and confidentiality
- Integrity in actions and access to systems and data


These ethical systems provide a useful starting framework, which may eventually grow into a modern equivalent of the Geneva Conventions for cyberwarfare behaviors and practices.



CHAPTER SUMMARY

This chapter has examined the existing treaties and conventions that make up the laws of warfare, including the Geneva Conventions and the UN Charter. It explored the role of cyberwarfare and traditional or kinetic military action in the context of those laws, and how cyberwarfare capabilities and methods go beyond their scope.

Those changes and similarities are well explained in the Tallinn Manual, a NATO-sponsored analysis of existing laws and rules of war. This chapter explored the Tallinn Manual to better understand common concepts and their application to cyberwar. Finally, this chapter looked at existing codes of ethics for information security professionals and military officers who may be called on to participate in computer network attack and defense actions to better understand the choices they may have to make about their participation in cyberwar.



KEY CONCEPTS AND TERMS

Civilian infrastructure	Jus in bello	Ruse
Cloud computing	Kinetic warfare	Sovereignty
Control	Mercenaries	Tallinn Manual
Jurisdiction	Nonkinetic warfare	Treachery
Jus ad bellum	Organ	

