2

Intelligence in Twenty-First-Century Conflict

The supreme art of war is to subdue the enemy without fighting.

Sun Tzu, The Art of War

Our idea of what constitutes conflict has changed substantially in the past two decades. The conflicts that have erupted around the globe bear little resemblance to the interstate wars of the previous millennium. These new types of conflicts have been referred to by terms such as shadow wars or hybrid wars.1 One writer on the subject has described them as follows:

The state on state conflicts of the 20th century are being replaced by Hybrid Wars and asymmetric contests in which there is no clear-cut distinction between soldiers and civilians and between organised violence, terror, crime, and war.2

Chinese People’s Liberation Army colonels Qiao Liang and Wang Xiangsui in 1999 published a book entitled Unrestricted Warfare. In it they described their vision of a new form of conflict. Their book may have gotten more attention in Washington than it ever did in Beijing, but it was prophetic about what was to come in this century. Its main points were as follows:

(1) If in the days to come mankind has no choice but to engage in war, it can no longer be carried out in the ways with which we are familiar.

... the degree of destruction is by no means second to that of a war, represent(ing) semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare.

War which has undergone the changes of modern technology and the market system will be launched even more in atypical forms. In other words, while we are seeing a relative reduction in military violence, at the same time we definitely are seeing an increase in political, economic, and technological3 violence.
If we acknowledge that, the new principles of war are no longer “using armed force to compel the enemy to submit to one’s will,” but rather are “using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one’s interests.”

Conventional wars that involve large-scale engagements (such as the first and second Persian Gulf Wars) undoubtedly will continue. But much of intelligence today is about what are being called shadow wars, hybrid wars, or unrestricted conflict, which are not conventional and which extensively involve nonstate actors. The conflict in Syria/Iraq, the Afghan insurgency, the Ukraine crisis, and Boko Haram’s activities in Africa all exemplify this type of conflict. Law enforcement must deal with another type of unconventional conflict with transnational criminal enterprises. Transnational corporations must also deal with types of competition that business leaders thirty years ago would not recognize—including conflicts with customers and suppliers.

The types of conflicts themselves aren’t new. Guerrilla warfare dates back to ancient history; when faced with superior military force, an opponent inevitably moves to what has been called asymmetric warfare (a form of conflict that exploits dissimilarities in capability between two opponents). Guerrilla warfare was common in ancient China. Nomadic and migratory tribes such as the Scythians, Goths, and Huns used forms of it to fight the Persian Empire, the Roman Empire, and Alexander the Great. Similar tactics were used with success during the American Revolution and the Civil War. Niccolò Machiavelli in his book *The Prince* described all of the types of conflicts that are prevalent today, along with advice on how a national leader should deal with them.

**Nature of Twenty-First-Century Conflict**

The unique features of twenty-first-century conflicts—the ones that distinguish them from conflicts of past eras—have been shaped by globalization and the Internet. The two dominant characteristics involve the increased roles of networks and of nonstate actors in conflicts.

**Networks**

John Arquilla and David Ronfeldt of RAND Corporation described the idea of conflict between networks in their discussion of the impact of new communications and information technologies on military structures, doctrines, and strategies. They coined the term *netwar* and defined it as a form of information-related conflict, in which opponents form networks—also known as network-centric conflict. Specifically, Arquilla and Ronfeldt use the term to describe the “societal struggles” that make use of new technologies. The technologies they discuss were (and are) available and usable anywhere, as demonstrated by the Zapatista netwar back in January 1994: A guerrilla-like insurgency had developed in Chiapas, Mexico, led by the Zapatista National
Liberation Army. The Mexican government's repressive response caused a collection of activists associated with human-rights, indigenous-rights, and other types of nongovernmental organizations (NGOs) elsewhere to link electronically with similar groups in Mexico to press for nonviolent change. What began as a violent insurgency in an isolated region mutated into a nonviolent but disruptive social netwar that engaged the attention of activists around the world and had both nationwide and foreign repercussions for Mexico. The Zapatista insurgents skillfully used a global media campaign to create a supporting network of NGOs and embarrass the Mexican government in a form of asymmetric attack.6

Two decades later, in 2015, netwars were active in many regions of the world involving states, commercial entities, and other nonstate actors. In the Middle East, two major protagonists headed major networks in conflicts across the region:

- Iran was providing financial and military support to Hezbollah in Lebanon, to the regime of President Bashar Al-Assad in Syria, to the Zaydi Houthis in Yemen, and to Shiite militias in Iraq. Under the banner of Shiite solidarity, Iran also provided nonmilitary aid for industrial projects, madrasas, mosques, and hospitals in Shiite regions.
- Saudi Arabia, for its part, provided weaponry and funding to Sunni combatants in Syria, Iraq, and Yemen. Riyadh also deployed its military forces to support the Sunni cause in some cases. In 2011, it sent armored units into Bahrain to quell the pro-democracy rallies of the country's Shiite majority. During 2015, it led aerial attacks against the Zaydi Houthis.7

Criminal, insurgent, and terrorist groups have their own networks that conduct economic, political, and military activities on a global scale. Their ability to access financing, advanced weaponry, and recruits extralegally makes them powerful players in international affairs—more powerful than many states, in fact. Their skill in adapting to changing environments and to threats also exceeds that of most governments.

Networks, of course, have been used in conflicts for centuries. The American Revolution, after all, was a kind of netwar: Thirteen colonies were supported by France on one side; and Great Britain was supported by loyalists and some American Indian tribes on the other. Both world wars involved conflicting networks of states. But the importance of networks in conflicts has increased because of the new tools discussed later in this chapter and the enhanced role of nonstate actors, discussed next.

**Nonstate Actors**

Participants in twenty-first-century conflicts are not just governments. Many networks, as the preceding section indicates, are comprised of nonstate
actors. They include criminal groups, commercial enterprises, and many other types of NGOs. The Zapatista netwar described earlier indicates the importance of nonstate actors. Some commercial enterprises, for example, engage in illicit arms traffic, support the narcotics trade, and facilitate funds laundering. While states continue to be the principal brokers of power, increasingly there exists a profusion of nonstate centers of power that include unconventional and transnational organizations. These groups operate with their own rules and norms that differ markedly from the traditional rules observed by governments.⁸

Intelligence is concerned with the following major nonstate actors:

- **Insurgents.** A few recent conflicts illustrate the direction of twenty-first-century conflicts where insurgency is involved: the conflict between Israel and Hezbollah in Lebanon, 2006; the emergence and expansion of Daesh (referred to in the United States as the Islamic State of Iraq and the Levant [ISIL] or Islamic State of Iraq and Syria [ISIS]) beginning in 2011; and the Ukrainian separatist conflict that began when Russia seized the Crimea in 2014. These conflicts had several features in common. The insurgents made use of sophisticated weaponry such as armor and antiarmor weapons and surface-to-air missiles. They had support from states not directly involved in the conflict—with Iran supporting Hezbollah, some Gulf states supporting Daesh, and Russia supporting Ukrainian separatists.

- **Transnational criminal enterprises.** These Mafia-like groups engage in narcotics and human trafficking, piracy, illegal trafficking in natural resources and wildlife, cybercrime, and funds laundering—in the process destabilizing regions, subverting governments, and operating in failed states. The largest such group, Japan’s Yamaguchi-gumi, engages in drug trafficking, gambling, and extortion. Yamaguchi-gumi has an annual revenue of about $80 billion, more than the gross domestic product of countries such as Libya and Cuba.

- **Individuals.** Networks must communicate to plan and execute operations, giving intelligence an opportunity to discover their plans. The “lone wolf” poses a different problem. When a single person rather than a unit or an organization is the key player, the intent to commit a terrorist act is far more difficult to identify. Most lone-wolf attacks are by followers of radical movements—often, but not exclusively, radicalized Islamists. For example, in July 2011, Norwegian right-wing extremist Anders Breivik killed 77 people in a bomb attack in Oslo followed by a shooting spree on a nearby island.

These nonstate actors use strategies and tactics designed to outmaneuver their conventional opponents. They use creative techniques that don’t involve
direct encounters with superior force and increasingly make use of advanced
technologies and tools of conflict. What’s new is the nature of the tools, lethal
and nonlethal, that can be used and the strategies that accompany them. These
are different enough from past methods that they change the nature of the
game. Let’s take a closer look at some of them.

**Tools of Conflict**

In the 1960s the U.S. military defined four top-level levers through which a
state exercises its power to influence events or deal with opponents. The mili-
tary called these levers *instruments of national power*: political, military, eco-
nomic, and psychosocial. Over the years, there have been several iterations of
this breakdown. Some authors divided “psychosocial” into psychological and
informational. In the business world, the levers are almost the same: political,
economic, environmental, and social. The argument has been made that tech-
nology is a fifth major instrument of national power, or of business power, on
the same level as the other four. Technology certainly is a factor (and often the
critical factor) in intelligence assessments.

Four such instruments are used widely today: diplomatic (or political),
information, military, and economic, usually referred to by the acronym DIME.
We’ll use the DIME construct in this book, though the name is misleading;
these are also instruments of power for organized groups other than states.

**Diplomatic**

The diplomatic or political instrument has a long history. While the dip-
lomatic instrument is an old one, it remains a powerful tool for mustering the
others—information, military, and economic. The most effective instrument
wielded by the United States against the Soviet Union during the Cold War
arguably was diplomatic: the organization of military and economic alliances
aimed at thwarting Soviet expansion and limiting Soviet influence worldwide.
This was the execution of the U.S. “containment” policy.

The use of diplomacy to form networks and alliances against opponents
still can be highly effective. In 2014 the United States led in the formation of
a coalition with European Union and international partners to impose stiff
sanctions on Russia for its actions in Ukraine. For their part, opposing non-
state actors can use political tools to covertly infiltrate and subvert uncoopera-
tive or hostile governments. For the conflicts described in this chapter, each
group has some level of backing by a nation-state.

**Information**

The information instrument has been the game-changer in twenty-first-
century conflicts, enabling more effective use of the other tools as well as being
a tool for mobilizing supporters, recruiting fighters, and obtaining funding.

Worldwide, both the participants in conflicts and the events they create
receive extensive media attention. The international press covers all such
conflicts in detail, often taking a sensational view. And the participants leverage this coverage to promote their views and rally international support.

The Internet has become the most prominent vehicle for applying the information instrument. Most visible is the surface web, which is used for obtaining information and for communication. But nonstate actors make extensive use of the deep web—the part not indexed (and, therefore, not searchable) by search engines. Terrorists and transnational criminal groups especially use darknets within the deep web to communicate clandestinely.

Cyber operations are used extensively by nonstate actors who rely on both the deep web and social media in the surface web to conduct such operations. These operations are useful for raising funds, distributing propaganda, discrediting opponents, recruiting followers, and targeting critical infrastructure or opposing leadership for the application of other instruments. Daesh has become a leading example of how to use cyber operations effectively in conflicts. It has used social media to recruit jihadists in the United States and Europe and to encourage lone-wolf attacks on military and law enforcement personnel.

Cyber operations often are used to attack; to shape social and political views, to attack infrastructure or economies, or to conduct hacking attacks on web sites. In that role, they arguably could be considered as a type of military tool (the application of a different type of force). But because they are linked so closely to other information tools, offensive cyber operations are treated in this book as an information instrument.

**Military**

We’ve seen many advances in the capabilities of military units, thanks to the application of technology. Two classes of weaponry have been developed and improved over the past few decades and now have changed the nature of the military instrument.

One class is precision weaponry, which until recently was a tool used only by advanced powers. Its value derives from its use in precisely attacking high-value targets and minimizing collateral damage. Highly accurate air-to-ground missiles, guided by laser designators, Global Positioning System (GPS), or both, have been the tools of choice in counterterrorism operations. Increasingly, precision weapons that include surface-to-air missiles have been acquired by less advanced countries and non-state actors.

The opposite class involves indiscriminate weapons, often used as instruments of terror or in a form of asymmetric warfare used against advanced military powers or hostile populations. This weapons class includes improvised explosive devices (IEDs); suicide bombers; rockets launched against urban areas; and chemical, biological, nuclear, and radiation weapons.

**Economic**

International organizations and coalitions rely on sanctions and embargoes as economic instruments against states that defy international norms, using the
political instrument to enforce them. Nonstate actors rely on the military instrument to acquire economic benefits—piracy, kidnappings, and hostage-taking being examples. And both state and nonstate actors rely on economic tools to conduct financial transactions that subvert the international rule of law.

The economic instrument uses the Internet extensively, both for traditional financial transactions and for the informal transactions that characterize an undercover economy. Currency manipulation and international trade in illegal goods are examples:

- The Hawala informal system for transferring money long has existed in the Middle East, North Africa, and India. It comprises a large network of funds brokers that functions on mutual trust. Hawala operates in parallel to but separate from international banking and financial channels. It now relies heavily on the Internet for communicating the details of funds transfers.
- Since its invention in 2008, the bitcoin has become an important online payment mechanism. This virtual currency relies on peer-to-peer transactions. While it is widely used in legitimate financial transactions, the bitcoin also serves those who want to avoid having their transactions tracked.
- The dark web is a primary vehicle for online payments of all types that participants wish to conceal. Darknet markets sell drugs, software exploits, and assassination and fraud services, among others. The Silk Road case, described below, illustrates how the practice works.

Between 2011 and 2013, Ross Ulbricht led a team that created and managed the largest online black market for illegal drugs in the world. Called “Silk Road,” the website operated as a darknet, concealing itself and its users by relying on the Tor browser. (Tor protects the identity, location, and transactions of a user by bouncing communications through a distributed network of relays run by volunteers across the globe.) Silk Road sold illegal goods, mostly drugs such as heroin, methamphetamine, MDMA, and LSD, using only bitcoins for transactions. During its nearly three years in operation, the Silk Road team collected 614,305 bitcoins in commissions—worth approximately $80 million at the time of Ulbricht’s arrest in October 2013. In May 2015, Ulbricht was sentenced to life in prison for his role in Silk Road.

**Synergy of the Tools**

The examples in this chapter mostly involve military actions, where military is defined in a broad sense to mean “use of armed force.” But many conflicts of intelligence interest today are not military. And both military and nonmilitary conflicts make use of diplomatic, economic, and information dimensions, usually applied in a synergistic fashion. The negotiations between Western powers and Iran on constraining Iran’s nuclear weapons program in 2014–2015 are an example of nonmilitary conflict that encompassed all of
these factors. Both sides developed political coalitions for support—with the United States, European powers, several Middle Eastern countries, and some NGOs on one side; and the Iranians, Russians, and some NGOs on the other. Economic levers included trade embargoes against Iran. Iran in turn used its economic and political connections to evade sanctions to some extent. Both sides used the information instrument to rally political and social support: The Western powers played to fears of a nuclear-armed Iran, and the Iranian government for its part stoked anger at the United States and appealed to Iranian pride about independence from foreign pressure. Information conflict within the Middle East also targeted social divisions, with Iran rallying Shiite Muslims to its cause, and Saudi Arabia leading the Sunni Muslims in opposition. The military element was there, of course, in the hint that if negotiations didn’t succeed, then a physical attack on Iran’s nuclear material production facilities might be in the cards.

**The Conflict Spectrum**

Military organizations commonly define three levels of conflict: strategic, operational, and tactical. Policymakers, law enforcement, and businesses experience similar levels of conflict. The types of intelligence are often defined to mirror these three levels, though like the conflict levels themselves, the lines between types of intelligence are often blurred. Sometimes, it is difficult for the customers of intelligence to tell where they are in the spectrum; the activities indicated in Figure 2-1 occasionally are all going on at the same time. Conflict, here, does not necessarily mean physical conflict. It can refer to business competition, negotiations, or the normal process of law enforcement.

Against any opponent in a conflict, three successive levels of action can be taken. One can attempt to **prevent**, **deter**, or **prevail**. Figure 2-1 shows a spectrum that includes these levels of action. Preventive operations tend to be strategic and to focus on planning. Actions intended to deter or prevail are mostly tactical; they transition from planning to managing the developing crisis and executing the plans. *This is not a clean division.* It illustrates the type of activity often conducted at a specific level. But deterrence, for example, could occur at the strategic, operational, or tactical level.

**Prevent**

Executives, policymakers, and operations organizations first try to prevent a disadvantageous situation from developing. Examples include preventing

- The opponent from organizing and acquiring momentum
- The opponent from acquiring or developing a capability, a strategy, or a new weapons system
- The opponent from making an unfavorable decision
- The opposing negotiations team from taking a certain position
- A country from acquiring a nuclear weapon
- Juveniles from forming or joining gangs
Prevention can also include making an existing situation more advantageous, for example, by encouraging an opponent to reverse an unfavorable decision that has been made; rolling back an opponent’s existing capability; or inducing the opponent to abandon a favorable position or pull out of a contested area.

**Deter**

Deterrence is used when it is too late for prevention. Examples include the following:

- Deterring an attack
- Deterring the use of a capability or weapons system
- Deterring the opponent from escalating or aggravating a crisis
- Creating uncertainty that induces the opponent to be cautious
- Deterring gang members from criminal activity

Prevention keeps a situation from becoming unfavorable; deterrence focuses on an opponent’s potential actions to resolve an already unfavorable situation in its favor.

**Prevail**

When all else fails, the goal is to resolve the conflict on favorable terms. Examples include the following:

- Defeating the opponent in armed combat
- Creating a perception that an insurgent opponent is losing, in order to deny recruiting and popular support
- Destroying the opponent’s weapons of mass destruction or sources of revenue
- Taking market share away from the opponent in commerce
- Arresting and incarcerating criminals
- Dismantling international criminal networks
- Imposing trade embargoes

**Figure 2-1  The Conflict Spectrum**
Until September 11, 2001, when terrorists attacked the World Trade Center and the Pentagon, the U.S. Department of Defense's Central Command (CENTCOM) was focused primarily on prevention and deterrence regarding the Taliban and Al Qaeda in Afghanistan. After 9/11, CENTCOM moved quickly into operational planning and then into tactics for defeating its opponents. In 2015, France could not prevent Islamic terrorists from targeting the humor magazine Charlie Hebdo, but it could deter them with police guarding the magazine’s headquarters. And when deterrence failed in the January 7, 2015, attack on Charlie Hebdo that killed twelve people, the French were able to move to the prevail stage, subsequently killing the two terrorists who were responsible.

The Function of Intelligence

Twenty-first-century conflicts call for a different pattern of intelligence thinking, if we in the intelligence business are to provide the support that our customers need. The next few chapters detail how to provide such support. As an introduction, though, we’ll spend the rest of this chapter focusing on the role that intelligence has always played and still must play in dealing with these types of conflicts. Then we’ll look at how the methodology works.

The Nature of Intelligence

Intelligence is about reducing uncertainty in conflict. Because conflict can consist of any competitive or opposing action resulting from the divergence of two or more parties' ideas or interests, it is not necessarily physical combat. If competition or negotiation exists, then two or more groups are in conflict. There can be many different levels, ranging from friendly competition to armed combat. Context determines whether another party is an opponent or an ally. Parties can be allies in one situation, opponents in another.14 For example, France and the United States are usually military allies, but they sometimes are opponents in commercial affairs.

Reducing uncertainty requires that intelligence obtain information that the opponent in a conflict prefers to conceal. This definition does not exclude the use of openly available sources, such as newspapers or the Internet, because competent analysis of such open sources frequently reveals information that an opponent wishes to hide. Indeed, intelligence in general can be thought of as the complex process of understanding meaning in available information. A typical goal of intelligence is to establish facts and then to develop precise, reliable, and valid inferences (hypotheses, estimations, conclusions, or predictions) for use in strategic decision making or operational planning.

How, then, is intelligence any different from the market research that many companies conduct or from traditional research as it is carried out in laboratories, think tanks, and academia? After all, those types of research are also intended to reduce uncertainty. The answer is that most of the methods
of intelligence research are identical to those pursued in other fields, with one important distinction: In intelligence, when accurate information is not available through traditional (and less-expensive) means, then a wide range of specialized techniques and methods unique to the intelligence field are called into play. Academics are unlikely to have intercepted telephone communications at their disposal as a means for collection and analysis. Nor must a lab scientist deal routinely with concealment, denial, or deception.

Because intelligence is about conflict, it supports operations such as military planning and combat, diplomatic negotiations, trade negotiations and commerce policy, and law enforcement. The primary customer of intelligence is the person who will act on the information—the executive, the decision maker, the combat commander, or the law enforcement officer. Writers therefore describe intelligence as being actionable information. Not all actionable information is intelligence, however. A weather report is actionable, but it is not intelligence.

What distinguishes intelligence from plain news is the support for operations. The customer does (or should do) something in response to intelligence, whereas television viewers typically do not do anything in response to the news—though they may do something about the weather report. The same information can be both intelligence and news, of course: Food riots in Somalia can be both if the customer takes action on the information.

We said earlier that intelligence supports decision making across the spectrum of conflict. Intelligence, like operations, can be broadly defined at the top level as being strategic, operational, or tactical—so long as it is recognized that the divisions among them are blurred, and all three types can occur at the same time.

**Strategic Intelligence**

Strategic intelligence deals with long-range issues. For the military customer, strategic intelligence is produced for the senior leadership. It is used to prepare contingency plans, determine what weapons systems to build, and define force structures. For national customers generally, strategic intelligence is used to create national policy, monitor the international situation, and support such diverse actions as trade policymaking or national industrial policymaking. For corporations, it typically supports strategic planning, market development plans, and investment.

Whether building a target model from scratch or updating an existing one, an analyst must spend much time because there are lots of options. One can consider many possible scenarios, and the situation can evolve many different ways because strategic intelligence takes a long-term analytic view.

Strategic intelligence involves much the same process in government and business. Both look at the political structure and alliances of opponents, both create biographical or leadership profiles, and both assess the opponent’s technology.
Strategic intelligence is tougher than tactical intelligence, which we’ll discuss later. The analyst has to command more sophisticated analytic techniques. The process is similar or identical to that used for tactical intelligence but usually is more complex because of the longer predictive time frame. One problem is that the intelligence analyst is seldom able to put aside short-term tactical support to customers while developing a clientele having the long-term view.\(^1^6\) The analyst needs a champion in the customer suite to support him or her in strategic intelligence because tactical intelligence, dealing with immediate issues, usually consumes all available resources.

The essence of strategic intelligence is best understood in terms of the methodology used in strategic planning, known as SWOT:

- **Strengths**
- **Weaknesses**
- **Opportunities**
- **Threats**

The SWOT methodology is the basis of all strategic planning, though it is not always made explicit. New techniques for strategic planning pop up from time to time, but SWOT always underlies them.

**Operational Intelligence**

Operational intelligence focuses on the capabilities and intentions of adversaries and potential adversaries. It is defined as the intelligence required for planning and execution of specific operations. Operational intelligence therefore has to be predictive also.

At the national level, once policy has been established, the intelligence customers have to develop operational plans to execute the policy or to carry out the strategic plan. A few examples of the many possible ones are included here:

- It could involve planning for diplomatic negotiations. Intelligence then has to determine what the opposing negotiators want and what they will agree to.
- It could involve planning for a trade embargo. Here, intelligence must determine what sanctions are likely to be effective and what the target country can do to defeat sanctions.
- It could involve support to research and development (R&D) that will result in new weapons systems. R&D support has to be predictive, because it can take years for a development program to produce a new weapons system, and the system must be effective in that future environment.
Operational intelligence in diplomatic efforts could support, for example, planning the negotiation of an arms reduction treaty. In law enforcement, operational intelligence is defined as intelligence that supports long-term investigations into multiple, similar targets. In this definition, operational intelligence is concerned primarily with identifying, targeting, detecting, and intervening in criminal activity. It might, for example, support planning for the takedown of an organized crime syndicate. In business intelligence, it might support a campaign to gain market share in a specific product line.

The SWOT method that we examined for strategic planning is useful also for operational planning, though the emphasis is different. When you’re making plans, you are more focused on opportunities that derive from opponent weaknesses. A key point to remember is that the opponent’s strengths translate directly to your threats, and the opponent’s weaknesses provide your side with opportunities. Intelligence has the job of identifying those strengths and weaknesses.

For the military, operational intelligence has a specific name. The Army and Air Force call it intelligence preparation of the battlefield. The Navy likes to use the term intelligence preparation of the battlespace. Whatever the name, the process involves the detailed analysis of the enemy, surface conditions (terrain or sea conditions), and weather within a specific geographic area. It starts before the next operation and continues throughout combat operations. Its goals include understanding the adversary’s forces, doctrine, tactics, and probable courses of action, together with the physical and environmental characteristics of the target area.

Intelligence preparation of the battlefield is a recent name for a very old technique. At the battle of Marathon in 490 B.C.E., the Greeks determined the only feasible route for a Persian attack (think of geospatial intelligence here), and stationed their forces in a narrow valley along that route that maximized the advantages of the Greek phalanx formation taking the Persian cavalry out of the battle.

The military coined the term operational intelligence to describe intelligence that is primarily used by combatant and subordinate joint force commanders and their component commanders. It keeps them abreast of events within their areas of responsibility and estimates when, where, and in what strength an opponent will stage and conduct campaigns and major operations. But operational intelligence also is used by national-level, law enforcement, and business entities to support operational planning, as we’ll discuss in this chapter.

The best operational intelligence is predictive. Analysts have to visualize the enemy’s tactical formations, the effect of terrain and weather, and how the enemy might alter his formations to adapt to specific terrain and weather. But predicting an opponent’s future actions is difficult. Analysts lack complete information because of gaps in collection capability or because of the opponent’s denial and deception. The job of intelligence is, again, to reduce uncertainty by assessing capabilities and likely courses of action.
To continue with the SWOT concept, the opportunities assessment typically supports targeting. During the targeting process, intelligence selects targets in accordance with the military commander’s guidance, objectives, and the results of the intelligence preparation of the battlespace. Targets may be either physical targets, such as bridges and command centers, or functional targets, such as enemy command and control capability. Two historical examples of how the process works are the 1990–1991 coalition operations called Desert Shield/Desert Storm, and the 2006 conflict between Hezbollah and Israel in Lebanon. These two examples illustrate the challenges of operational intelligence in more recent decades as compared with earlier conventional conflicts.

**Operation Desert Shield/Desert Storm.** During Operation Desert Shield and throughout the air operations of Desert Storm, U.S. Navy and Army special operations personnel and force reconnaissance Marines established a series of observation sites along the border between Kuwait and Saudi Arabia. These sites were used for continuous visual and signals intelligence (SIGINT) surveillance of Iraqi forces across the border. Information from these ground sites was combined with imagery and SIGINT collected by coalition aircraft in the theater. The process provided an intelligence picture of the locations, combat capability, and intentions of Iraqi units in Kuwait, as well as indications of the vulnerability of Iraqi forces along the Iraq/Saudi Arabian border west of Kuwait. This thorough intelligence preparation of the battlespace contributed significantly to the subsequent successful ground offensive to liberate Kuwait.19

Operation Desert Shield/Desert Storm was a coalition operation, so allied forces were also customers of the intelligence that supports operational planning. The trend is to such joint actions. These present a number of challenges that are associated with intelligence sharing, discussed later in this book.

**Lebanon War, 2006.** On July 12, 2006, Hezbollah militants in Lebanon fired rockets at Israel, as a diversion for an ambush on an Israeli patrol. During the ambush, Hezbollah fighters killed three Israeli soldiers and captured two. Hezbollah then demanded the release of Lebanese prisoners in Israel in exchange for the captives. Israel responded by attacking Hezbollah and Lebanese civilian targets, followed by imposing an air and naval blockade and conducting a ground invasion of Lebanon. Hezbollah in turn launched more rockets into Israel and began a campaign of guerrilla warfare in southern Lebanon.

The Israelis’ operational intelligence preparation for the conflict was strikingly different from the coalition preparation for Desert Shield/Desert Storm. Hezbollah fighters were well equipped with combat and communications gear, were well trained, and used tactics designed to maximize their advantages—fighting from well-fortified positions in urban areas with advanced weaponry that
included anti-tank guided missiles. They focused on inflicting casualties on the Israeli Defense Forces (IDF) because of a perceived unwillingness of the Israelis to accept casualties. Both made use of the media and NGOs such as Human Rights Watch and Amnesty International to garner international support—with Hezbollah pointing to Israeli attacks on civilians and the civilian infrastructure, and Israel arguing that Hezbollah was using civilians as human shields. After the conflict ended with a cease-fire on August 14, 2006, both sides claimed victory. Though Israel appeared to have won in terms of relative casualties, Hezbollah emerged relatively intact with an enhanced reputation from having stood up to the much more powerful IDF.

Israeli intelligence support failed in several areas. They targeted bunkers that Hezbollah had deliberately set up as decoys, missing most of the 600 concealed ammunition and weapons bunkers in the region. Their targeting of Hezbollah leaders in Beirut and their communications infrastructure also failed. Hezbollah, for its part, demonstrated a SIGINT capability that allowed it to anticipate Israeli moves and succeeded in “turning” Israeli human intelligence (HUMINT) assets in southern Lebanon to feed back misleading information to Israeli intelligence.20

To conclude the SWOT concept, operational intelligence has to assess threats. For example, intelligence must give an accurate picture of the opponent’s missile threat by calculating where the missiles might go, how quickly the opponent can fire them, and which of your own forces are in the threat envelope.

Operational intelligence to support law enforcement has its own name, and it very much resembles intelligence preparation of the battlespace in a civil environment. It is called intelligence-led policing. The term intelligence-led policing originated in Great Britain. The Kent Constabulary developed the concept after experiencing substantial increases in property-related offenses during a time when it was dealing with budget cuts. The constabulary believed that only a few people were responsible for a large percentage of burglaries and automobile theft. Its hypothesis—which subsequent events proved to be valid—was that police would have the best effect on crime by focusing on these most common offenses.21

Operational intelligence to support intelligence-led policing can take several forms. Analysts can anticipate crime trends so that law enforcement can take preventive measures to intervene or mitigate the impact of those crimes. Intelligence that supports, for example, planning to shut down a gang operation or a narcotics ring would be operational. As an example, to help fight terrorism and domestic extremism, the California Department of Justice examines criminal group characteristics and intervention consequences to determine which groups pose the greatest threat to the state.

Operational planning in business can take many forms, as can the nature of the intelligence to support such planning. Planning a campaign to reduce...
the market share of a competitor requires good knowledge of the competitor's weaknesses. Negotiations with suppliers or large customers require much the same sort of knowledge that is needed to support international treaty negotiations: what the other side has to have, and what it is willing to give up.

**Tactical Intelligence**

The military uses the term *tactical intelligence* to refer to quick-reaction intelligence that supports ongoing operations. As was true at the operational level, intelligence has a well-established role at tactical levels that is spelled out in military doctrine. This form of intelligence is associated with a concept that the U.S. military calls *battlespace awareness*. Tactical intelligence is used at the front line of any conflict. It is used by field commanders for planning and conducting battles and engagements. Tactical intelligence locates and identifies the opponent's forces and weaponry, enhancing a tactical commander's ability to gain a combat advantage with maneuver, weaponry on target, and obstacles. It allows tactical units to achieve positional advantage over their adversaries.22

Tactical intelligence to support the military became much more important during the 1990s because of weapons technology trends. The trend toward employing highly precise weaponry and operations placed a premium on highly accurate data. Intelligence systems that can geolocate enemy units to within a few meters became more important than before. The rapidly expanding field of geospatial analysis supports such surgical operations with mapping, charting, and geodesy data that can be used for the guidance of “smart” weapons.23

Add to that a new field of combat—cyber operations—that is still in development and may be poorly understood by some commanders. Surgical operations in the cyber world are at least as important as surgical operations in the physical world.

The result, as one author has noted, is that

Many of the new C4ISR systems (including national systems), and much of the effort and funds expended by the Intelligence Community since the Gulf War, have focused on providing direct, real-time support to forces engaged in combat by closing the “sensor-to-shooter” loop and to meeting the information needs of the senior-level commanders directing those operations. When there are American forces deployed in active military operations, as there have been on a near-continual basis since the end of the Cold War, the highest priority is now accorded to providing intelligence to support them.24

The dominance of U.S. capabilities for battlespace awareness has resulted in an added task for tactical intelligence. Targets on the battlefield typically exceed the number of available sensors and weapons that can be
used against them. Thus it is important to find and attack the most important targets. So, tactical intelligence has the job of identifying the enemy forces, systems, and activities that will yield the highest payoff in terms of disrupting enemy operations and reducing his combat effectiveness. Again, cyber operations have added a whole new dimension in disrupting enemy combat effectiveness.

Battle damage assessment (or combat damage assessment) could be considered the final stage of battlespace awareness. It includes not only physical damage assessment, but also functional damage assessment. Physical damage assessment quantifies the extent of damage to a material target. An example would be imagery indicating the center span of a bridge has been destroyed, thus severing an enemy resupply line. Functional damage assessment determines the disruption of operational targets by “nonkinetic” attack. For example, it would assess the effectiveness of electronic jamming on enemy command and control capabilities. Battle damage assessment relies heavily on quick-reaction intelligence, because the commander has to decide quickly what targets need to be attacked again.

Much of law enforcement intelligence also tends to be tactical in orientation. In the law enforcement world, tactical intelligence is defined as that which contributes to the success of specific investigations. But tactical intelligence is used every day in situations well removed from military actions and law enforcement, as the following example illustrates:

A satellite photo of the Earth spins slowly on a large plasma screen, with markers indicating the sources of online threats. At rows of computer workstations, analysts monitor firewalls and other online defenses. The displays, the layout, and the security guards all evoke the image of a war room—which it is, but for a new type of war.

This is Symantec’s war room. Here, a different type of intelligence analyst deals with junk e-mailers who are trying to stay one step ahead of filters and blacklists that block spam; of the hackers that constantly work to bypass bank firewalls; and of the viruses that can flow into thousands of computers worldwide in a few seconds.

Symantec maintains the war room to defend banks and Fortune 500 firms against cyber threats. This room was the front line of the battle against SQL Slammer as it surged through the Internet, knocking out police and fire dispatch centers and halting freight trains; against MSBlaster, as it clogged corporate networks and forced web sites offline; and against the graffiti viruses with such innocuous names as Melissa and I Love You.

The analysts in Symantec’s war room succeed in their tactical combat because they have shared models of viruses, worms, and Trojans instantly available. They model the operational patterns of East European organized crime
groups that use viruses such as SoBig to track a user’s keystrokes and to lift passwords and credit card numbers. They have models of the computers that are used to spread viruses. The great plasma screen itself displays a massive model of the Internet battlefront, where the beginning of new threats can be seen. Using these models and creating new ones on the fly, these tactical intelligence analysts can analyze and defeat a new virus in minutes.

Tactical intelligence is driven by the need for fast response in the military and law enforcement communities. For the national customers, it’s a classified form of the news; it’s called current intelligence.

**Summary**

Twenty-first-century conflicts have distinguishing features that are important for intelligence. They take a network form, the key players being nonstate actors that operate transnationally with the support or tolerance of governments. These actors may be criminal, insurgent, terrorist, commercial, or other nongovernmental organizations—or some combination. The resulting conflicts among such networks have been called netwars or network-centric conflicts.

As a result, much of intelligence today is about what are being called shadow wars, hybrid wars, or unrestricted conflict. Although these are not new types of conflicts, they present challenges because globalization and the ubiquitous Internet provide new tools for engaging in and prevailing in conflict.

The new tools of conflict can be thought of as dividing into four categories, known as the instruments of national (or organizational) power. These instruments are summarized in the acronym DIME: diplomatic (or political), information, military, and economic.

In these new conflicts, the primary job of all intelligence continues to be reducing uncertainty for the customers of intelligence. Intelligence analysis must support policy, planning, and operations across the spectrum of these new conflicts. The type of analysis and the speed with which it must be prepared and delivered to the customer vary accordingly. Analysis to support strategic intelligence tends to be in-depth research focused on capabilities and plans and to consider many possible scenarios.

Operational intelligence is more near-term, involving support to planning for specific operations. In military usage, it has a specific name: intelligence preparation of the battlefield (or battlespace). But operational intelligence also supports planning for economic and political activities such as trade embargoes and treaty negotiations.

Tactical intelligence support tends to be rapid response, or current intelligence, to support crisis management and plan execution; it is focused on the current situation and on indications and warnings. Again, the military gives it a specific name: battlespace awareness. Battle damage assessment is one phase of battlespace awareness. Much of the intelligence support to law enforcement and to countering cyber threats is tactical in nature.
Notes

3. In this context, *technological* refers to the use of information technology.
10. A darknet is a private network overlayed on the web that relies on connections between trusted peers.
13. JCS Joint Pub 2-0, “Joint Doctrine for Intelligence Support to Operations,” Chapter III.
15. Ibid.
18. JCS Joint Pub 2-0, Chapter III.
22. Ibid.
23. Geodesy is concerned with the size, shape, and gravitational field of the Earth, its coordinate systems, and reference frames.
24. Jeffrey R. Cooper, Curing Analytic Pathologies [monograph], Center for the Study of Intelligence (December 2005), 32.

Copyright ©2017 by SAGE Publications, Inc.
This work may not be reproduced or distributed in any form or by any means without express written permission of the publisher.