Intelligence in the Age of Contested Norms and Persistent Disorder

The violent conflicts that have erupted throughout the world in the past two decades bear little resemblance to the interstate wars of the previous millennium. These new types of conflicts are often referred to by terms such as hybrid wars. In 2003, one of Australia’s most prolific writers on international security, Alan Dupont, characterized the change succinctly:

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.

Even earlier than that, in 1999, Chinese People’s Liberation Army colonels Qiao Liang and Wang Xiangsui published a book titled 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:

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, representing 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, globalization, 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 are seeing a defined increase in political, economic, and technological violence.

The new principles of war are no longer exclusively “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.”

Copyright ©2020 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.
The U.S. Joint Chiefs of Staff (JCS) developed much the same perspective on conflicts for the next two decades, albeit using different terms, which form this chapter’s title. The JCS’s view was explained in the 2016 publication *The Joint Force in a Contested and Disordered World*:

**Contested norms will feature adversaries that credibly challenge the rules and agreements that define the international order.**

**Persistent disorder will involve certain adversaries exploiting the inability of societies to provide functioning, stable, and legitimate governance.**

Conventional wars that involve large-scale engagements (such as the first and second Persian Gulf wars) undoubtedly will continue. And great power competition shows no sign of disappearing. But much of intelligence today is about hybrid wars or unrestricted conflict, which are not conventional and which extensively involve nonstate actors. The recent conflict in Syria/Iraq, the Afghan insurgency, the Ukraine crisis, and Boko Haram’s activities in Africa all exemplify this newer type of conflict. Law enforcement must also deal with another type of unconventional conflict with transnational criminal enterprises. And transnational corporations must deal with types of competition that business leaders thirty years ago would not recognize—including conflicts with customers and suppliers.

The 2016 JCS publication summarized the major features of today’s conflicts. Violent ideological competition will continue to focus on the subversion or overthrow of established governments. Both state and nonstate actors will continue to rely on destabilizing methods, force, or the threat of force to advance their interests against opponents. Internal political divisions, environmental stresses, and external interference will combine to disrupt and bring down governments. Cyberspace will be a major contested arena in which these conflicts will take place.

The strategies and tactics themselves aren’t new. Unconventional warfare and subversion of existing governments date back to ancient history. When faced with superior military force, an opponent inevitably moves to what is called asymmetric warfare (a form of conflict that exploits dissimilarities in capabilities 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. Niccolo Machiavelli in his sixteenth-century work *The Prince* describes all the types of conflicts that are prevalent today, along with advice on how a national leader should deal with them. But Machiavelli could not have envisioned the nature of the tools being employed today, as discussed in the next two sections.
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 information technology. These two factors have increased the prevalence of networks and of nonstate actors in conflicts.

Networks

John Arquilla and David Ronfeldt of RAND Corporation describe 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 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.8

More than two decades later, in 2018, netwars were active in many regions of the world involving states, nonstate actors, and commercial entities. 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 President Bashar Al-Assad's regime 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.9
- 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. Beginning in 2015, it intervened in ...
Yemen against the Zaydi Houthis in what has become a proxy war with Iran.10

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.

And netwar has moved into social media, which has become a powerful tool for gaining an advantage in conflicts. The Russian operation to influence the 2016 U.S. presidential election is well known and publicized, but netwars are being carried on continuously in social media. One author has defined these types of political netwars as

> actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts (false amplifiers) aimed at manipulating public opinion.11

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 aided by guerrilla units and governments-in-exile. But the importance of networks in conflicts has increased because networks make better use of the tools of conflict discussed later in this chapter and because of the enhanced role of nonstate actors, discussed next.

**Nonstate Actors**

Participants in twenty-first-century conflicts are not all governments. Many networks, as the preceding section indicates, are composed of nonstate actors. They include criminal groups, commercial enterprises, and many other types of nonstate actors. 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 money 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. Intelligence is most concerned with the following major nonstate actors:

- **Insurgents.** A few examples illustrate the direction of twenty-first-century hybrid warfare in which insurgency was key: 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 the Islamic State of Iraq and Syria (ISIS)) beginning in 2011; and the Ukrainian separatist conflict that began when Russia seized Crimea in 2014. These all had several features in common. The insurgents made use of sophisticated weaponry such as armor and antitank 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 organizations engage in narcotics and human trafficking, piracy, illegal trafficking in natural resources and wildlife, cybercrime, and money laundering—in the process destabilizing regions, subverting governments, and operating in failed states. The largest such entity for many years, Japan’s Yamaguchi-gumi, engages in drug trafficking, gambling, and extortion. Yamaguchi-gumi’s annual revenue at one point was about $80 billion, more than the gross domestic product of countries such as Libya and Cuba. In recent years, the Yamaguchi-gumi has fragmented and fallen into decline, but Russian Mafia groups continue to thrive under Vladimir Putin’s regime and have extensive international operations.

- **Individuals.** Networks must communicate to plan and execute operations, giving intelligence an opportunity to discover their plots. 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 terrorists are followers of radical movements—often, but not exclusively, radicalized Islamists. As a counterexample, Norwegian anti-Muslim right-wing extremist Anders Breivik killed 77 people in July 2011 during a bomb attack in Oslo followed by a shooting spree on a nearby island.

A recent example of netwar involving both state and nonstate actors that expanded dramatically in 2018 is the one between Turkish president Recep Tayyip Erdoğan and Muslim cleric Fethullah Gülen.

Nonstate actors rely on strategies and tactics that often are not available to governments. The use of terror weapons such as improvised explosive devices
Part I | The Process, the Participants, and the Product

During the 1980s, Turkish cleric Fethullah Gülen founded and led a powerful movement that opposed secular elements in Turkey. His supporters exercised influence in the country’s political and justice systems, and the Gülen movement had expanded worldwide to include religious schools, charities, and media outlets. During this time, the Gülen movement grew into perhaps the largest Muslim network in the world. Called Hizmet (Turkish for “service”), it was loosely organized, with no formal structure and no official membership. Yet, it developed a following in the millions, and the funding it garnered was measured in billions of dollars.

Gülen also developed close ties with the Turkish Justice and Development Party (AKP) and its leader, Prime Minister Recep Tayyip Erdoğan. Erdoğan wielded political power; and Gülen supporters became entrenched in the Civil Service, police force, prosecutors’ offices, and judiciary. But, in 2013, the alliance between Gülen and the Turkish government began to disintegrate. The two split when Gülen criticized Erdoğan’s crackdown on protesters in May of that year. Erdoğan subsequently began a campaign to purge Gülen supporters from the Turkish government.

In 2016, a Turkish military faction attempted to overthrow now-president Erdoğan’s government. The coup failed; subsequently, approximately 50,000 people were reportedly arrested and 170,000 accused of complicity in the coup attempt. Those arrested or charged included many associated with the Gülen movement. President Erdoğan accused Gülen of instigating the coup and directed the closing of Gülen schools in Turkey, seizing the movement-owned newspaper Zaman and several companies that had ties with Gülen.

The aftermath of the coup has been a full-scale netwar between the Erdoğan government and the Gülen movement—which we'll revisit later in this chapter, after an introduction to the tools used in netwar.

(IEDs), assassinations, and public executions of captives are not options for most governments. Insurgents also use creative techniques that don’t involve direct encounters with superior force and increasingly make use of advanced technologies and tools of conflict. The tools themselves are not new. What is new is the way that the tools, lethal and nonlethal, are used and the strategies that accompany them. These are different enough from past methods that they change the game, often to the advantage of the nonstate actor. Let’s take a closer look at some
tools that are available to both state and nonstate actors—though the two may use the tools differently—before returning to the Erdoğan-Gülen case.

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 military called these levers instruments of national power: political, military, economic, and psychosocial. Over the years, there have been several iterations of this breakdown. For example, some authors divided “psychosocial” into psychological and informational.¹³ In the business world, the levers are almost the same: political, economic, environmental, and social. The argument has been made that information technology is a fifth major instrument of national power, or of business power, on the same level as the other four. Information technology certainly is a factor (and often the critical factor) in intelligence assessments.

Four such instruments are used widely today and applied in new ways by nonstate actors: diplomatic (or political), information (which replaces “psychosocial” in the 1960s definition), military, and economic, usually referred to by the acronym DIME. We’ll use the DIME construct in this book, recognizing that these are also instruments of power for organized groups other than states. Note that the DIME instruments are identical to the “military, political, economic, and technological” forms of violence identified by colonels Qiao Liang and Wang Xiangsui.

Diplomatic

The diplomatic (or political) tool has a long history. It nevertheless remains a powerful one 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 the European Union and other international partners to impose stiff sanctions on Russia for its actions in Ukraine. Beginning in 2006 and continuing into 2018, the United States joined an even larger coalition, including the United Nations, in imposing a series of trade and financial sanctions on North Korea because of its nuclear weapons and missile testing. Nonstate actors can use political tools to covertly infiltrate and subvert uncooperative or hostile governments, usually as part of a network that includes nation-states. In the conflicts described in this chapter, each group has some level of backing by a nation-state.
Information

The information instrument is old. Propaganda has been used in conflicts for centuries. But its new form, information technology, has been the game-changer in twenty-first-century conflicts, enabling more effective use of the other tools as well as being a method for mobilizing supporters, recruiting fighters, and obtaining funding.

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

The Internet has become the dominant vehicle for applying the information instrument. Most visible is the surface web, which is routinely used for disseminating and 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 and the dark web, both of which function within the deep web, to communicate clandestinely.

Cyber operations are used extensively by nonstate actors who rely on social media in both the surface web and the deep 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 became a leading example of how to use cyber operations effectively in conflicts. It employed 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. They are employed to mislead and confuse opponents, shape social and political views, attack infrastructure or economies, or conduct hacking attacks on websites. 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 available only to advanced powers. Its benefit derives from its use in precisely attacking high-value targets while minimizing collateral damage. Highly accurate air-to-ground missiles, guided by laser designators, the Global Positioning System (GPS), or both, are today’s tools of choice in counterterrorism operations. Increasingly,
precision weapons that include surface-to-air missiles have been acquired by less advanced countries and nonstate actors.

The other 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 IEDs and vehicle-borne IEDs (VBIEDs); suicide bombers; rockets launched against urban areas; and chemical, biological, nuclear, and radiation weapons.

Another challenge is developing, in the form of a combination of the two threats: unmanned aerial vehicles (UAVs, or drones) that can be precisely guided to a target and deliver an IED or an incendiary, chemical, or biological weapon. Drones are widely available, relatively cheap, and easily fitted with explosive devices. Their use by terrorist and insurgent groups is becoming commonplace. During July 2018, Russia reportedly dealt with forty-five drone attacks on its Khmeimim Air Base in Syria.

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—for example, through piracy, kidnappings, and hostage taking. 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, Bitcoin has become an important online payment mechanism. This virtual currency relies on peer-to-peer transactions. Although it is widely used in legitimate financial transactions, Bitcoin (along with a variety of other major cryptocurrencies such as Ethereum) also serves those who want to avoid having their transactions tracked.

- The dark web—the clandestine side of the deep 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.
Synergy of the Tools

Many examples in this chapter involve military actions, where military is defined in a broad sense to mean “use of armed force.” But interests of intelligence today are not strictly military. And almost all types of 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 each 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 focused on 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. Within the Middle East, the information lever was used to target social divisions, with Iran rallying Shiite Muslims to its cause, and Saudi Arabia leading the Sunni Muslims in opposition. The negotiations ended with a nuclear deal struck in 2015 between Iran and six world powers: the United States, the United Kingdom, Russia, France, China, and Germany.

Synergy of the tools is an essential characteristic of netwars. Let’s revisit the Erdoğan versus Gülen case for an example of just how that works.
The Erdoğan-Gülen netwar illustrates how a number of the instruments are employed.

On its side, the Turkish government has wielded political power—successfully pressuring governments in twenty countries to shut down Gülen movement schools, and revoking passports and using organizations such as Interpol to obtain the arrest and deportation of its Turkish opposition in sixteen countries.19 Within Turkey, it has made extensive use of the military instrument (primarily law enforcement) to arrest or intimidate opponents. It has put continuing pressure on the United States to extradite Gülen (who has resided in Pennsylvania since 1999). In 2017, according to a Wall Street Journal article, U.S. Special Counsel Robert Mueller was investigating an alleged meeting between former White House national security adviser Michael Flynn and senior Turkish officials, during which they allegedly discussed an offer by the Turks to pay $15 million if Flynn and his son would arrange for Gülen to be deported to Turkey.20

One of the persons arrested after the 2016 coup attempt was Andrew Brunson, an American pastor who had lived in Turkey for years. The Turkish government claimed that Brunson was a Gülen supporter; it’s more likely that he represented a bargaining chip, possibly for the extradition of Gülen. The U.S. government had pressed Turkey since 2016 for Brunson’s release. In August 2018, citing the Brunson case as a factor, the U.S. government imposed steep tariffs on Turkish steel and aluminum—allowing Erdoğan to make use of the informational instrument, rallying Turks behind his government by claiming Turkey was a victim of economic warfare.21 (The Turkish government released Brunson in October 2018.)

The Gülen movement lacks the diplomatic and military instruments that the Turkish government can wield. So, its response has been to rely primarily on economic and informational instruments. The movement works less visibly than its opponent, and its use of these instruments is not widely documented. Most Gülen media outlets in Turkey have been closed, but the movement continues to have an extensive media presence elsewhere in the world. And it appears to have adequate funding to continue its operations. Unconfirmed reports suggest that the movement’s 130-plus charter schools in the United States are a source of funding,22 and the Turkish government has pushed the U.S. government to investigate or close Gülen-affiliated schools. As a result of the 2018 political, economic, and informational conflict between Turkey and the United States, it appears that Gülen has (at the moment) a new and powerful ally in the continuing netwar.
The Function of Intelligence

Twenty-first-century conflicts call for an evolving pattern of intelligence thinking, if we in the intelligence business are to provide the support that our customers need. The next few chapters outline 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 conflicts in the age of contested norms and persistent disorder. Chapter 3 will address how the intelligence process itself has changed.

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 does not necessarily include physical warfare. If competition or negotiation exists, then two or more groups are in conflict. There can be many distinct levels, ranging from friendly competition to armed combat. Also, context determines whether another party is an opponent or an ally. Parties can be allies in one situation, opponents in another. 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 prefers to conceal. This definition does not exclude the use of openly available sources, such as hard-copy media (newspapers and journals) or the Internet, because competent analysis of such open sources frequently reveals information that the other side 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, both are intended to reduce uncertainty. The answer is that most of the methods used in intelligence 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, a wide range of specialized techniques and methods unique to the intelligence field are called into play. Academics, for example, are unlikely to have intercepted telephone communications at their disposal in conducting 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, cyber operations, 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 consumers typically do not do anything in response to the news—though they may do something in response to the weather report. The same information can be both intelligence and news, of course: For example, food riots in Somalia can be both if the customer acts on the information.

Intelligence 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 potentially occur at the same time.

### Strategic Intelligence

Strategic intelligence deals with long-range issues. For the military customer, strategic intelligence is produced for 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 guidance.

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 to produce than tactical intelligence, which we’ll discuss later. The analyst must 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. The analyst must spend more time because there are lots of options. One has to consider many possible scenarios, and the situation can evolve in different ways; strategic intelligence, therefore, takes a long-term analytic view.

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. The analyst needs a champion in the customer suite to support him or her in strategic intelligence because tactical intelligence, dealing with immediate issues, can easily consume 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.

Strategic intelligence using SWOT has a long history in competitive intelligence. Businesses routinely turn to their strategic planning staff for SWOT assessments, because looking at strengths and weaknesses means looking internally. But looking at opportunities and threats means looking externally; and for that, companies rely on their competitive intelligence unit. Governmental intelligence units also look at the “OT” part of SWOT. And not just for strategic intelligence, but also for operational and tactical intelligence, as discussed in the following sections.

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. The military coined the term to describe intelligence that is used primarily 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.

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. Consider the following examples of operational plans:

- It could involve planning for diplomatic negotiations. Intelligence then must 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 might do to defeat sanctions.
- It could involve support to research and development (R&D) that will result in new weapons systems. R&D intelligence 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 involve, 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 context, operational intelligence is concerned primarily with identifying, targeting, detecting, and intervening in criminal activity. Operational intelligence might, for example, support planning for the takedown of an organized crime syndicate. In competitive intelligence, it might support a campaign to gain market share in a specific product line.

The SWOT method for strategic planning is useful also for operational planning, though the emphasis is different. Whereas strategic planning is more policy oriented, operational planning is focused more on threats and 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 U.S. 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), 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 really just 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 to maximize the advantages of the Greek phalanx formation while taking the Persian cavalry out of the battle.

Customers prefer operational intelligence that is predictive. Analysts have to visualize or model the enemy's tactical formations, the effect of terrain and weather, and how the enemy might alter formations to adapt to those specific conditions. But predicting an opponent's future actions is difficult. You will always 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.

Military operational planning also requires identifying enemy units that are high priority to attack. Intelligence officers with special training in targeting usually have this role. During the targeting process, they select and prioritize targets in accordance with the military commander's guidance and objectives and the results of the intelligence preparation of the battlefield (or 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. The two examples illustrate the difference between operational intelligence in conventional twentieth-century warfare and that of more complex twenty-first-century conflicts.
Operation Desert Shield/Desert Storm represents a conventional twentieth-century conflict, both in time and in type, against an opponent who fought conventionally. It was a coalition operation, so allied forces were also customers of the intelligence that supported operational planning. Although the trend is toward such joint actions, they present several challenges that are associated with intelligence sharing, discussed later in the book.

The Lebanon case represents a twenty-first-century conflict, both in time and in type. It illustrates the challenge of conducting operational intelligence in a situation characterized by netwar, contested norms, and persistent disorder.

BOX 2.4  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.

Operation Desert Shield/Desert Storm represents a conventional twentieth-century conflict, both in time and in type, against an opponent who fought conventionally. It was a coalition operation, so allied forces were also customers of the intelligence that supported operational planning. Although the trend is toward such joint actions, they present several challenges that are associated with intelligence sharing, discussed later in the book.

The Lebanon case represents a twenty-first-century conflict, both in time and in type. It illustrates the challenge of conducting operational intelligence in a situation characterized by netwar, contested norms, and persistent disorder.

BOX 2.5  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.
Operational intelligence to support law enforcement has its own name. It is called intelligence-led policing. The term originated in Great Britain. The Kent Constabulary developed the concept after experiencing substantial increases in property-related offenses during a time when they were dealing with budget cuts. The constabulary believed that only a few people were responsible for a significant percentage of burglaries and automobile theft. Their 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.30

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 and how best to deal with them.

The Israelis’ operational intelligence preparation for the conflict was strikingly different from the coalition preparation for Desert Shield/Desert Storm. Israeli operational 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 communication 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.29

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 antitank 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 sides made use of the media and NGOs such as Human Rights Watch and Amnesty International to garner international support—Hezbollah pointed to Israeli attacks on civilians and the civilian infrastructure, and Israel argued that Hezbollah was using civilians as human shields. After the conflict ended with a ceasefire on August 14, 2006, both sides claimed victory. Though Israel appeared to have won in terms of relative casualties, Hezbollah emerged almost intact with an enhanced reputation for having stood up to the much more powerful IDF.
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 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 must 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 by identifying immediate opportunities and threats (SWOT, again). As was true at both the strategic and operational levels, 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 maneuvers, weaponry on target, and obstacles. It allows tactical units to achieve positional advantage over their adversaries.31

Tactical intelligence to support the military became much more important during recent years because of weapons technology trends. Employing highly precise weaponry and operations places a premium on highly accurate data. Intelligence systems that can geolocate enemy units to within a few meters have become more central to military maneuvers. 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.32

The result, as one author notes, is that

> 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.33

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 their operations and 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 is about the disruption of a target’s effectiveness, whether by kinetic or nonkinetic attack. For example, it would assess the effectiveness of electronic jamming or a cyber attack on enemy command-and-control capabilities. Battle damage assessment relies heavily on quick-reaction intelligence, because the commander must 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. 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 is called current intelligence. And tactical intelligence is used every day in situations well removed from military actions and law enforcement, as the following example illustrates.

**BOX 2.6 Symantec’s Tactical Intelligence**

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 twenty-first-century conflict.

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 criminal hackers who constantly work to bypass bank firewalls; and of the viruses that can flow into thousands of computers worldwide in a few seconds.

Symantec maintains this control center to defend banks, Fortune 500 firms, and millions of its software users against cyber threats. It 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 websites offline; and in 2017 against a new wave of ransomware such as Petya and WanaCrypt0r.

(Continued)
Although the preceding sections discuss three distinct types of intelligence, they actually form a continuum and sometimes all three intelligence activities are going on at the same time. They also inform each other. Operational and tactical intelligence, for example, often shape strategic thinking. And, for their part, operational planners frequently rely on strategic intelligence in preparing their plans.

**SUMMARY**

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

As a result, much of intelligence today is about hybrid wars or unrestricted conflict. Although these are not new, they present challenges because globalization and the ubiquitous Internet provide new tools for engaging in and prevailing in conflict. These tools may be thought of as dividing into four categories, known as the instruments of national (or organizational) power. The instruments are summarized in the acronym DIME: diplomatic (or political), information, military, and economic.

In current 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 conflict spectrum. To do so, it identifies the opponents’ strengths and weaknesses and the consequent opportunities and threats to the customer’s interests, captured in the acronym SWOT. 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. Its time reference is long term.

• 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). Operational intelligence also supports planning for economic and political activities such as trade embargoes and treaty negotiations. In law enforcement, it supports intelligence-led policing to identify or anticipate crime trends.

• Tactical intelligence support tends to be rapid response, or current intelligence, to support plan execution or crisis management; it is focused on the immediate situation and on indications and warning. 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, to business, and to countering cyber threats is tactical in nature.

CRITICAL THINKING QUESTIONS

1. Choose an existing major crime cartel, narcotrafficker, insurgent, or street gang to consider. From that group’s perspective, who are your opponents? Identify the strengths and weaknesses of the opponents, and the opportunities and threats that they pose. What weapons and tools (DIME) do you have available to use against them? What types of intelligence and specific intelligence do you need to sustain your organization in the conflict? How will you obtain it?

2. Consider the same group that you analyzed in Question #1. Diagram the group’s likely organizational structure or network. You will have to make assumptions about the elements of the network, deducing them from the group’s operations and results. Not all members will turn up in an online search.

3. The case titled “Netwar: Erdoğan versus Gülen” has a partial list of the DIME instruments employed by each side. Identify them. From sources available to you, can you provide a more complete list of the organizations and tools used by each side in their netwar?

4. Identify three to five norms on the Internet that can be exploited (contested) by state or nonstate actors to achieve disorder.

NOTES

3. In this context, technological refers to the use of information technology.
6. Ibid., iii.
14. A darknet is a private network overlay on the web that relies on connections between trusted peers.
24. Ibid.
31. Ibid.
32. Geodesy is concerned with the size, shape, and gravitational field of the Earth, its coordinate systems, and reference frames.
33. Jeffrey R. Cooper, Curing Analytic Pathologies [monograph]. Center for the Study of Intelligence (December 2005), 32.