Chapter 3
The Impact of the Information Revolution

One of the most challenging issues for international security today is the information revolution. Although no single assessment can investigate every implication of this issue, this chapter highlights potential opportunities and dangers posed by the information revolution that will challenge the international security arena.

The chapter begins by focusing attention on the nexus of the information, technology, and defense sectors. It then explores ubiquitous cell phone connectivity, transparency, and cyber warfare—all trends in networked communications that indicate the information revolution is no longer limited to the West but involves every corner of the world. The next section looks at the threats posed by hackers. It suggests that the tendency toward overclassification actually intensifies these threats. The following section examines threats caused by the shift from hierarchical systems to networks and decentralized edge networks of hackers that operate beyond the reach of traditional control mechanisms. The responses to these threats will require standardizing international laws, sharing intelligence, and widening edge-to-edge contact at relatively low levels among nations, organizations, corporations, and individuals.

The use of the Internet by al Qaeda and its sympathizers is the topic of the next section, which offers a glimpse of the ways in which communications among people on the edge can turn into violence. Internet design precludes eliminating such conversations, and thus it is wiser to exploit them. The ensuing section considers space-based capabilities integral to the information revolution, including the global positioning system, video over the Internet, and global communications. Understanding the potential of space is essential in the development of a global information network. The final section, on the relationship of technology and the changing character of war, investigates how genetics, robotics, and nanotechnology have advanced through the information revolution. Technology, like information itself, will soon present both benefits and risks for public and private entities as well as corporate and individual actors using commercially available technology. And a peer competitor may arise from any of these areas.

The Information Environment

Thirty years ago, U.S. defense planners envisioned a military transformation in which war would be conducted by weapons infused with electronics and driven by information. Then, 15 years ago, graduate students created the first visual Web browser known as Mosaic that popularized Internet access. Today, the relationship between technology, information, and defense shapes the world and U.S. national security policy (see figure 3–1). Three trends in this information revolution are relevant to strategic concerns: ubiquitous cell phone connectivity, transparency, and cyber warfare.

Ubiquitous Connectivity

Just a few years ago, half of the world population had never heard a dial tone. In 2008, the number of people who own cell phones exceeded the number who did not. Places such as Africa and rural India, barely touched by the Industrial Revolution, are plunging headlong into the information revolution with the help of cell phones. Even where cell phone ownership is relatively expensive, many have found ways to enjoy its benefits through the work of institutions such as Bangladesh's Grameenphone that help micro-entrepreneurs lend phones on a per-call basis.

The full effect of ubiquitous person-to-person communications can only be guessed at, but some effects are already noticeable. Farmers and fishermen, for instance, are now plugged into local and even international markets on a nearly real-time basis—their incomes have risen 5 percent on average from simply being able to sell into the best markets. Rural parents are much better connected to their children who have moved to the city. Evanescent trading and employment opportunities can be communicated far more easily, lubricating the accommodation to the inevitable shifts wrought by globalization. Large political groups are capable of mobilizing their membership in protest (as they have done in Burma, Thailand, and the Philippines).

One would think that the ubiquity of cell phones—in 5 years Iraq (or at least that part controlled by Saddam Hussein) went from zero to 12 million cell phones—would be the insurgents' friend. With these devices, insurgents could acquire a command and

control system that would rival U.S. and Iraqi government forces. Of late, the contrary has proven true. Indeed, insurgents have targeted cell phone towers and eliminated service in places such as Ramadi (Anbar Province), but motivated locals were using cell phones to provide intelligence on insurgent identities and whereabouts

Moreover, cell phones offer ways to combat terrorism by identifying dangerous individuals. The phones are hardware-dependent and need a handset and subscriber information module (SIM) that can be matched to cell towers and switches. Every time a cell phone is used, switches identify the phone and SIM card of the caller, the phone called, and the location of each phone through the global positioning system (GPS) and triangulation. Moreover, if it was possible to connect the identity of individuals with SIM chips, phone companies could learn more about customers. Although such knowledge can be used for nefarious purposes, it also could deliver government services, prevent illicit use of cell phones, inhibit insurgent use of cell phones, and provide forensic evidence and immediate intelligence to security forces. Influence over the cell phone screen and favorable billing policies can make it easier to establish neighborhood watch groups and provide feeds from approved sources. In more affluent countries, mobile communications are proliferating. Adolescents are more likely to use phones for texting than for talking. Phones with GPS capabilities can locate anything from the nearest Starbucks to the local hospital. Between the wired Ethernet, wireless short-range Bluetooth, medium-range WiFi, and long-range WiMax, it is hard to roam beyond Internet range. Social networking sites based on Web 2.0 such as Facebook, MySpace, LinkedIn, and Twitter make it possible to reach out and touch *everyone*.

Who will benefit more from this trend: we or our enemies? Once there were fears that terrorists would disrupt the Internet because it is a symbol of open societies. Instead, they have adopted it as a means of communication and recruitment. Tens of thousands of jihadist Web sites have sprung up to transmit messages, motivate sympathizers, and recruit new adherents. Many terrorists drawn to Iraq, and to a lesser extent Afghanistan, were attracted through these sites. However, the digital footprint left by jihadist use of the Internet has been a way of tracking would-be terrorists in the United States and Great Britain. Sunni jihadists and al Qaeda in Iraq among others use the Internet to influence supporters and threaten enemies. Fortunately, data can differentiate one group from another and provide intelligence on group dynamics.

Transparency

U.S. forces in Vietnam could enter and leave a village before anyone outside the area was aware of their presence. Given today's ubiquitous and instantaneous nature of communications systems, such opacity has disappeared. In fact, it is unclear if anything on a future urban battlefield can be kept secret for longer than it takes to establish a cell phone connection.

Global transparency is also increasing. The launch of several satellites with resolutions better than 1 meter makes quality imagery available to anyone with a credit card. Both Google and Microsoft supply the Internet with imagery via the Internet-based application, Google Earth. Although the U.S. Government has persuaded these companies to reduce the resolution of some pictures and established right of first refusal on real-time battlefield shots, the overall result is the same: no place on Earth can be hidden. Imagery has been used by nongovernmental organizations to monitor disaster sites and hold governments accountable for sins of omission and commission. The ability to get the word out with cell phones and the Internet makes official secrets difficult to maintain. In the case of Zimbabwe, where repression of political protesters and the press would have gone unnoticed, transparency and connectivity revealed the problems internationally. Nevertheless, determined authorities can resist the global transparency of the Internet. In the People's Republic of China, censorship remains effective despite the efforts of individual users to circumvent its restrictions.

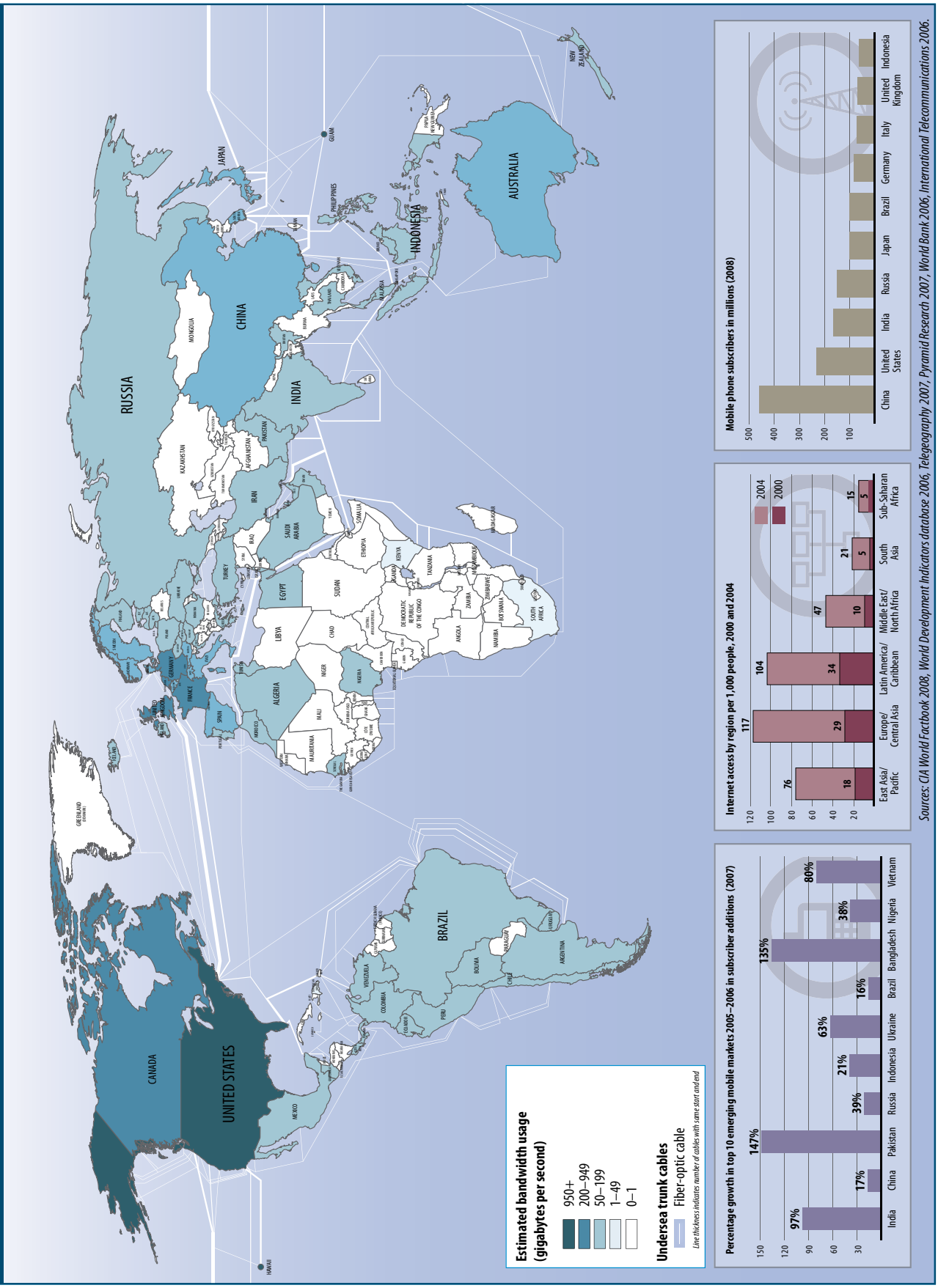
Some believe that the Internet proliferates ideas, which in turn leads to greater openness and equality. Studies have indicated that when people have more freedom to choose among media outlets, they lean toward those that reinforce prior beliefs. As a result, established ideas are less often challenged or modified. Ironically, the openness of the Internet has permitted repression as well as justice to be voluntarily outsourced; witness the recent case of a Chinese student in America who protested repression in Tibet. She was identified by pro-Beijing peers over the Internet, and her family in China was harassed and threatened.

Cyber Warfare

Information technology and the Internet are increasingly vulnerable to cyber attack. Much of what once was controlled by hardware and physical infrastructure is now controlled by software, a medium that is infinitely malleable by other software, which makes cyber attack increasingly possible and harder to trace. Emblematic of this problem was the distributed denial-of-service attack that constricted access by

Continued on p. 57

Figure 3–1. Information Revolution



Sources: CIA World Factbook 2008, World Development Indicators database 2006, Telegeography 2007, Pyramid Research 2007, World Bank 2006, International Telecommunications 2006.

Al Qaeda, Its Sympathizers, and the Internet

Al Qaeda, together with its affiliates and sympathizers, uses the Internet to spread its views on Salafi jihadism and reestablish the caliphate. The group regards attention by the media and *dawa*, or proselytizing, as indispensable to jihad, of equal or greater importance than violence. The Internet is central to its plans because it is the only medium to which it has unrestricted access.

Thousands of Web sites have content sympathetic to Salafi jihadists. For those people who seek information, these sites contain text, video, audio, graphics, chat rooms, bulletin boards, discussion groups, and even computer games. Discussions range from casual dialogue to highly sophisticated conversations about theology, politics, strategy, tactics, and weapons. Approaches range from the abstract to the practical expressed in styles from the polemical and exhortatory to the dispassionate and intellectual. The material is designed for a variety of functions, including planning, propaganda and radicalization, training, education, and social purposes.

Within the Salafi jihadist movement, there are two countervailing tendencies: one consciously prefers uniformity and another stands for individual action. Much Salafi jihadist activity is associated with one of several terrorist or insurgent groups that produce and disseminate branded material to the world. These groups are concerned with attribution and authority. Many have affiliated regional production centers that produce videos, magazines, information bulletins, and even poetry. For instance, as-Sahab Media is affiliated with al Qaeda central, while al-Furquan Media is associated with the Islamic State of Iraq. Their products are disseminated through Internet clearinghouses such as the al-Fajr Media Center or Global Islamic Media Front. Such clearinghouses typically serve as outlets for various production organizations. They also serve as guarantors of the authenticity of the material, which appears on elite, access-controlled Web sites such as al-Ekhlaas and al-Hesbah. Typically, about 90 percent of the products are text, about 9 percent video, and the balance is audio, graphic, and other forms. The majority of the text items can be classified as military reports and policy statements, while the rest are periodicals, books, and essays.

The balance of the material on the Web sites of Salafi jihadists is commentary and discussion springing from established as well as homegrown sources. The latter appear on many al Qaeda–affiliated and independent sites. Freelance self-styled intellectuals can draw significant followings on controlled access and quasi-official sites. Occasionally, original documents can gain substantial traction, as occurred with "Jihad in Iraq: Hopes and Dangers," which appeared in 2003 under the byline of an unknown group (never heard of again) and may have inspired the Madrid train bombings. This combination of controlled information and spontaneous contributions poses serious security dangers.

Effects

Young people are disproportionately likely to seek information, entertainment, and social contacts on the Internet. Moreover, an increasing amount of jihadist material is available. Thus, in the past few years the Internet, rather than physical locations, has become the venue for training young recruits who eventually commit acts of terrorism.

Radicalization on the Internet generally does not happen as a result of people reading official publications from as-Sahab, the Global Islamic Media Front, or some other organization. People are actually galvanized to radicalism and eventually action through the less formal aspects of the Internet, including discussion forums, chat rooms, email, and listserves.

In addition, ideas that could pass for military doctrine influence the global jihad. These ideas, such as the work of the Salafi jihadist strategic thinker Abu Musab al-Suri, strongly influence the actions of organized groups such as al Qaeda, but also reach informal parts of the Salafi jihadist world. They are particularly important in dealing with leaderless resistance.

Squelch or Exploit?

Individual extremist Web sites come and go. However, the prospect of impeding online Salafi jihadist discourse is minimal at best. Often the sites are hosted by nations with free speech protections. Furthermore, intelligence gain-loss calculations may suggest that it is preferable for some to operate. The prospects for making a serious dent in such Web sites with technical sabotage are low. The Internet was designed for almost endless growth, and it provides nearly anonymous communication. Indeed, some jihadist forums have been hosted on numerous uniform resource locators, but they continue to thrive. Historically, it was impossible to squelch the spread of subversive materials before the Internet came along. The experience of the Soviet Union with samizdat and extensive penetration of the speeches of Ayatollah Khomeini in Iran under the Shah by means of cassette tapes are two examples. Notwithstanding the success of taking down main Web sites that carried al Qaeda messages, at the end of the day exploiting communications may be more productive than trying to interrupt them.

Continued from p. 54

major Web sites in Estonia. In reaction to Estonia's decision in 2007 to move a Russian World War II memorial, protestors mobilized thousands and possibly millions of computers to send packets to Web servers of government offices and national banks, knocking many offline. With few exceptions, these computer owners were unwitting participants in the attack. Unlike previous attacks using slow-moving "bots," these cyber tactics were organized and executed in hours. No one knows their origin: Estonia blamed Russia, Russia stonewalled Estonia, and the only person convicted was an Estonian of Russian descent.

State-sponsored cyber attacks are becoming increasingly commonplace. China is often cited as being in the vanguard of cyber espionage. Recently, state-sponsored hackers placed malicious code on computers when users downloaded material from suspect Web sites or opened email attachments from seemingly reliable parties. Once ingested in a targeted computer, the code opens data files from the inside, sending terabytes of information to the hackers. Victims of this tactic were users worldwide including military bases, defense contractors, and private businesses. Hackers look for technical information, but since malicious codes cannot tell one type of information from another, they must search many haystacks to find the needle.

In response to attacks, the U.S. Government added measures to tighten information security in late 2007. The National Security Agency was made responsible for protecting civilian as well as military networks. As a result, the number of government gateways to the open Internet will be drastically reduced. Other forms of counterespionage and cyber defense are being explored, but it is unclear if such activities can be deterred. Moreover, if cyber espionage is ever declared an act of war, it will have world-changing implications.

Network insecurity will remain problematic in the future. As computers become more secure, hacker tools will improve. The key to network security will reside in reducing vulnerabilities. In the meantime, governments should rely on primitive methods of security, including disconnecting critical systems from the outside world or refusing to use Web-based systems.

Understanding Cyber Attacks

Many people consider "computer network attacks" the domain of cyber-espionage and governments, with reviews restricted to highly classified environments. However, throughout the civilian arena, there are active, open source discussions about how to penetrate computer networks, and sophisticated penetration tools are available to anyone with Internet access. Nongovernmental actors have participated in real world attacks on governments, and unclassified laboratories exist to test new tools and train those responsible for Internet security.

A search on the term *computer network attack* generates some 17,600,000 references on Google[1] while *computer hacking* generates about 5,390,000.[2] Many of the sites generated by a search for *computer network attack* focus on policy, history, and concepts. In contrast, many of the sites generated by the term *computer hacking* display and teach specific tools for mischievous or malevolent activity. These malevolent sites run the gamut from "point and click" procedures that can be used by anyone with a computer mouse to powerful tools for experienced hackers.[3]

From a government perspective, classifying such tools and procedures is important to protecting sensitive activities and network vulnerabilities. Yet from the hacker's perspective, the information is readily available and thousands of users already know how to attack networks. For this reason, the government needs to be careful that it does not overclassify information about capabilities that already are available to opponents. Such knowledge is necessary for adequately defending networks from mal-intents.

Lessons from DEFCON

The DEFCON convention is held every summer in Las Vegas and bills itself as "the largest underground hacker convention in the world." This is a serious event—typically including more than 80 presentations in 4 or 5 parallel tracks, which often run well into the evening. It brings together talented people with

DOD

Team that developed first large-scale digital computer, the IBM automatic sequence controlled calculator, poses in front of the massive computer

diverse viewpoints. Topics discussed there can affect cyber security and information-sharing initiatives, so it is worth summarizing some points from recent years. Given the scope of each DEFCON, the observations that follow reflect only a part of the activities at the conferences, but they give some idea of the scope and sophistication of the subjects addressed.

In 2006, three of the focus areas were:

- "Owning" an organization through the BlackBerry. (This was a physical access issue, reinforcing the point that all portable devices that can access networks need to be protected by passwords. BlackBerries are reasonably secure electronically.)
- The dramatic increase in the *attack surface* (their term) afforded by the proliferation of wireless devices such as WiFi and WiMax. (Many security personnel do not understand the detailed data structures of these systems, and their spread contributes to increased use of wireless by people who do not pay much attention to security.)
- The dramatic increase in the attack surface caused by the transition to Internet Protocol (IP) version (v) 6. (Once everything is native IP v6, it will be more secure than IP v4, but during the transition, many do not understand that there are vulnerabilities in the complex header structure and packets tunneling between IP v4, and v6 stacks are immune from "deep packet inspection.")

Sourceforge.net

WiFi scanner in use at DEFCON, considered the world's largest underground hacker convention

In 2007, the focus was more on identity theft and data manipulation. The first point was that the real objective of hacking is getting not only root access to a computer, but also the data itself—stealing it, corrupting it, hiding it, or manipulating it. The ways to get to the data are through the people (stealing identities), their applications, their operating systems, and only then the computer itself. In this context, presentations put special emphasis on programs that allow someone to scan an individual's total Web presence, cross-reference his email accounts and address books, look at cookies, identify frequent correspondents (who might not inspect attachments closely) and so forth. Identity theft poses special challenges since it can be used to circumvent many technical network defense measures and also is a key ingredient in online criminal activity.

In 2008, emphasis included:

- Exploiting social software and social networks, primarily as a way of gathering information for identity theft and preparation for "custom-tailored, laser-focused attacks." Analytical programs such as "Satan" are particularly valuable for these purposes.[4] The point here is not to cast doubt on the value of social networks; they are an important feature of society, online and offline. In recognition of this, the Social Software for Security[5] initiative is looking for ways to encourage the government to take advantage of the energy and imagination being put into the development of social software by balancing functionality and security. "Risk management" (as opposed to "risk avoidance") in these environments is critical, but it is important to understand the tradeoffs.
- Hacking opportunities provided by increasing use of wireless. "Always-on" connections mean "always-on" vulnerabilities. Talks at the conference discussed very imaginative attacks, especially focused on "men in the middle" operations to misdirect unwitting participants from what they think are secure Web sites to insecure ones. Most people still do not appreciate how much risk they are at in unsecured "wireless hotspots" at places such as airports.
- Discussions of "Open Source Warfare": how to combine various tools to triangulate cell phone conversations with video coverage from low cost ($400), remote control helicopters to permit isolation, and potential targeting, of individuals.

■ Sophisticated social network attacks taking advantage of personal behaviors (for example, sending free iPhones to people in the mailroom and then using them to monitor an organization's network configurations).

Other DEFCON talks focused on things such as breaking into physical locks, compromising e-voting (seems distressingly simple in many cases), hacking the Boston subway system fare cards (good enough that the Metropolitan Boston Transit Authority sued to stop the presentation), compromising network data integrity, and hardware Trojans that showed low cost ways to make a "secure" router transmit data via largely undetectable infrared, radio frequency, or optical signals.

In sum, each annual DEFCON provides both interesting and troubling insights into a world of energetic, talented people devoted to getting at information and information systems that others try to protect. Though many of the techniques shown there may have been used by governments, all those discussed at the conference are available to anyone.

Georgia

In his research on the Russia-Georgia conflict, Evgeny Morozov, the Berlin-based founder of the news aggregator *Polymeme*, explored the possibility of launching an amateur cyber attack on the country of Georgia by setting out:

to test how much damage someone like me . . . could inflict upon Georgia's Web infrastructure, acting entirely on my own and using only a laptop and an Internet connection. If I succeeded, that would somewhat contradict the widely shared assumption—at least in most of the Western media—that the Kremlin is managing this cyber warfare in a centralized fashion. My mission, if successful, would show that the field is open to anyone with a grudge against Georgia.

With tools available online and a short program he wrote in a Microsoft Word document, Morozov developed programs to promote denial-of-service attacks. He then went to "Stop Georgia," a Web site that claimed to be linked to the hacker underground in Russia. This site offered target lists of sites that indicated disruption and also offered downloadable code to customize attack options that could be launched by clicking the button labeled "Start Flood." As Morozov discovered, "Within an hour I had become an Internet soldier. I didn't receive any calls from Kremlin operatives."[6]

The denial-of-service attacks explored by Morozov are less sophisticated and disruptive than would be possible with the kind of data manipulation, identity theft, or computer penetration described at DEFCON or available from hacker sites. However, the fact that the Russian campaign against Georgia included kinetic and cyber activities is likely to be typical of future military action. The ease with which Morozov launched attacks reflects the amount of malicious information on the Internet. It also points to the difficulty in distinguishing between *official* and *unofficial* activities. This ambiguity was evident in operations against Estonia in 2007.

Labs at IRMC

The Information Resources Management College (IRMC) at the National Defense University in Washington, DC, offers cutting-edge classes on a wide variety of cyber-related issues for chief information officers, chief financial officers, chief information security officers, and others. Its courses on information operations help dozens of leaders understand cyber-threats and prepare themselves for Service and joint assignments.

IRMC also has a set of laboratories covering areas such as information assurance, supervisory control and data acquisition systems, and virtual reality. These labs are built around internal networks,

U.S. Air Force (Adam M. Stump)

Vice Chairman of the Joint Chiefs of Staff General James Cartwright speaks at Air Force cyberspace symposium on importance of experimenting with cyber warfare implementation

isolated from the Internet but populated with Internet tools. As such, these labs are used for extensive experimentation. The information assurance lab, in particular, offers detailed opportunities for nonexperts to implant malicious code in software applications and operating systems within these closed networks using openly available hacking tools. It emphasizes the importance of robust information assurance approaches and trains students how to implement them.

The supervisory control and data acquisition lab offers similar experiences regarding control systems for powerplants and other critical infrastructures. The virtual reality lab provides experience in the increasingly important area of avatars and virtual interactions. These are currently used in gaming but are expected to become integral to the command and control systems of the future. Not surprisingly, recent DEFCON conventions have included sessions on hacking avatars.

Any senior official associated with computer network operations, defense, exploitation, or attack should visit these laboratories. At a minimum, the capabilities developed in the labs and online should be synthesized into informational manuals that can be provided at unclassified levels to help train those who are operating and defending our networks.

A wise man recently asked: "What is more strategically threatening to the U.S. military than our inability to manage information in a contested environment?" Being able to operate and defend our networks is hard enough even when threats are well understood. Attack options available to opponents from open sources should be examined aggressively and disseminated with minimal caveats to strengthen our defensive posture on all networks, including the unclassified networks so important to personnel, medical, and logistic activities. More sophisticated tools may be available within classified channels, but this should not keep officials from knowing what is available to adversaries. Regular reviews to make sure that information is not overclassified could be a good way to avoid this danger.

The importance of cyber security also needs to be understood by senior officials across the new administration, not just those directly associated with the networks themselves. It should be taught as part of core courses in Department of Defense educational institutions, not only as electives. Cyber security is an issue of serious nationwide importance—it must be the concern of policymakers and commanders, not just communicators and technical specialists.

New Threats, New Responses

Enabled by modern network technologies, power is "shifting to the edge." This shift is allowing decentralized networked groups to vie with traditional hierarchical structures. Globalized communications and computing infrastructure combined with collaborative software permit hostile nonstate groups—terrorists, criminals, rogue corporations, antiglobalization movements, hackers, and others that act on behalf of nations or other entities—to threaten international security and stability. Increasingly, security arrangements based on geographic borders, sovereign control, and unilateral response to global threats by individual nations are inadequate to counter such groups. U.S. national security strategy must embrace a decentralized, multilateral public health model against unknown threats. This model should be based on local monitoring of emerging threats, swarming global response to counter manifest attacks, and developing resilient capabilities to withstand and recover in their wake.

Organizational Network

Emerging social and peer networking technology is enabling new organizational structures that afford opportunities for novel patterns of generative and degenerative activities. Such developments, which are popularly known as Web 2.0 or the Web as platform, underpin the decentralized networks as distinct organizational forms that have advantages over the traditional hierarchies in terms of flexibility, adaptability, and responsiveness.

As a result, the power to generate potentially catastrophic effects by organizing, coordinating, or sharing dispersed resources is shifting from the center to the periphery. Decentralized groups can synchronize activity globally without regard to political borders or local government control. If the groups are hostile, security arrangements that rely on the assumption that sovereign nations are responsible for activities in their territory and among their subjects are inadequate.

In the first stage of Internet development in Web 1.0, individuals, organizations, information, or devices at the edge of a network interacted with central servers, providers, or other authorities on an essentially one-to-one basis that mimicked hierarchical arrangements. In Web 2.0, the edges interact directly on a many-to-many basis. Although Web 1.0 enabled asynchronous mediated communication among edge elements, Web 2.0 enables synchronicity of effort without control or formal organizational structure. Although this greatly reduces the overhead associated with centralized management controls—and thus enhances the power

and speed of networked groups by lowering barriers to participation from the edges—it eliminates accountability for undesirable actions. Both agency and action shifted to the periphery in Web 2.0, making it difficult to hold leaders responsible for actions of subordinates or sovereigns responsible for actions of citizens. This inability to hold someone accountable is problematic for existing security policies that rely on deterrence through symmetric counterforce and retaliation.

New Threats

Until recently, the ability to aggregate resources to threaten national interests or international stability would have required the resources or authority of a nation. Thus, current legal and other approaches to cyber threats hold nations responsible for actions by their citizens and rely on identifying leadership or structures of adversaries to assign responsibility. However, network technologies enable nonstate actors to operate without respect for laws, borders, or governments. Technologies enable such groups to threaten international peace and security without being held accountable.

One illustration of a networked-enabled threat was the cyber attack against Estonia in 2007. Angry over the removal of a Russian monument, an apparently self-organizing group essentially paralyzed the government and financial sector of Estonia through a massive distributed denial-of-service attack against critical cyber infrastructure. Whether these attackers acted on their own in a cyber *riot* or with active Russian involvement in a cyber *war*, an organized group was able to project power across international borders on a scale that previously could only be accomplished by nation-states. More importantly, these actors accomplished their attack virtually spontaneously and without exposing leaders who could be held accountable under existing security laws.

It is likely that nations will be increasingly subject to attacks of this kind, which cannot be easily attributed to identifiable adversaries. The attacks will come from both spontaneous, self-motivated mobs and externally instigated mobs allied with other entities to further their interests. The externally motivated mobs may be encouraged by nations, terrorist groups, or other hostile entities and become proxies or merely swayed as useful idiots. However, traditional deterrence or retaliation strategies probably will be inadequate against these kinds of threats.

While security policy can hold other nations responsible for actions by their citizens, it fails to deter groups without an organization when no one has jurisdiction over them or where responsibility or motivation is ambiguous. Such failures must be distinguished from those identified with failed states where sovereign control is inadequate to counter hostile or illegal activity occurring in defined geographical areas where local government is ineffective. Rather, the kinds of threats discussed here may easily originate in well-functioning nations. The organization of hostile groups will be ambiguous and responsibility will not be easily attributable under existing security policies and recognized laws without a new international framework addressing responsibility or rights to act in these circumstances.

New Strategies

International security and stability require rethinking strategies, realigning force structures, and adopting new models to leverage resources in response to emerging threats. To a certain extent, traditional counterinsurgency strategies are effective against hostile networks. But applying those strategies requires that the potential adversary is identified and its dynamics, motivations, and support are understood. In cases where group formation is hidden or attribution and motivation are ambiguous during or after an attack, a different strategy is needed. In this case, global security resources that are resilient in the face of local failures and can suppress threats anywhere in the world must be engaged quickly to identify and counter the attack.

Traditional strategies based on counterforce, deterrence, and retaliation against an identified adversary are no longer enough to protect against spontaneous, ambiguous, and unknown threats. Instead, national security policies should be global and include aspects of a public health model. This model involves quickly identifying new and previously unknown threats through syndromic surveillance, the isolation of and inoculation against outbreaks, information-sharing to prevent spread, resilience to recover from attacks, and the simple prevention of a known disease. The public health model accepts the occurrence of unknown pathogens that cannot be prevented and aims to contain outbreaks to prevent epidemics. It is premised on a multilateral network of local resources acting in concert to amass resources where and when they are needed.

Effectively countering hostile networks requires decentralized and flexible architecture based on dynamic partnerships and coalitions, including with erstwhile competitors or adversaries, that identifies emerging threats, brings resources to bear with local legitimacy, ensures resilience, and aids in recovery. The same trends in technology that empower hostile networks can provide for effective counterforce reorganization or realignment.

Technological advances can improve collective global responses without significant costs by changing the way that global resources and capabilities are managed. Multilateral resources can be leveraged by increasing the relative power of nations and entities to respond to nascent threats by improving information-sharing and by *swarming* in response to manifest threats. Collective security can be increased by leveraging both the means and the opportunities for "edge entities" to participate in synchronic action against common threats to international order.

To successfully counter hostile groups operating globally requires four capabilities:

- the ability to spot threats locally before they emerge globally
- the ability to work in concert with allied or congruent interests and cooperatively engage local resources
- the ability to assemble and apply appropriate (and legitimate) counterforce wherever and whenever it is required
- the ability to orchestrate these activities to respond in a consistent and timely manner across all potential domains.

No nation, not even the United States, can achieve these capabilities alone. Unilateral action can hamper threat awareness, undermine common interests and legitimacy, and create additional hostile groups. In an interdependent world, nations and other entities interact within the context of conflict, competition, and collaboration. This complex dynamic supplants the linear paradigm of peace/crisis/war/peace on which previous strategic arrangements were premised.

In areas where there is an explicit recognition of long-term shared interests, alliances created by treaties can be used to formalize collaborative roles in collective security agreements such as the North Atlantic Treaty Organization. In circumstances where threats mobilize and sustain common national interests, coalitions may be formed for purposes such as intervention in Afghanistan and Iraq.

Where potential collaborators are simultaneously in competition, or where threats are unable to sustain long-term alliances, collective security may only be possible through multilateral security arrangements in what is known as foreign policy by posse. To respond to threats that can emerge anywhere and at any time, nations must develop communities of common interest through networks that transcend hierarchical organizations. A first step in developing communities is harmonizing international and domestic laws and seeking common understanding of activities that should be opposed, such as terrorism, illegal trafficking, cyber attacks, and arms trafficking.

Regional, national, and local security services can be organized to facilitate collective action. A basic infrastructure is needed to maintain continuous situational awareness of global threats—surveillance and information-sharing—to replace the brittle, antagonistic, border-based perimeter security models. Universal standards for civil liberties and human rights also must be developed. And response mechanisms must be synchronized on a global scale. Resources must be shared not only to identify threats (intelligence) or respond to them in a timely manner (law enforcement and military), but also to resist or recover from attack where preemption is impossible (resilience, recovery, and relief). The latter capabilities would help ensure global resilience to catastrophic natural disasters, pandemics, and other unforeseen shocks to the international order.

Although the ability to organize dispersed networked resources for beneficial purposes has the potential of improving global social and economic development, it can be used by malevolent forces to challenge U.S. interests. To respond effectively to decentralized networks bent on harm, the international community must take advantage of these same network opportunities by decentralizing capabilities that increase power, flexibility, and resilience to respond. Instead of maintaining rigid and exclusive hierarchies of stovepiped capabilities in nations, communities of interest must be fostered to dynamically share intelligence, response, and recovery capacities. Static communities of interest based only on existing alliances, known adversaries, and exclusive sovereign response will not be sufficient.

To succeed, major powers such as the United States will have to lead by example by sharing power and collaborating with other nations, including those with which it has competed or even fought in the past. In return, those nations will incur shared communal responsibility to act against common threats. There is no future in a networked world without collective security arrangements that reconcile conflicting interdependencies when faced with emerging threats. Although the United States is poised to lead such an effort, it cannot dictate one. It will have to work with others to maintain international security and stability by globally shifting counterforce to the edge.

Technology and the Changing Character of War

Unique technological advances are occurring in genetics, robotics, information technology, and nanotechnology (GRIN). Of particular interest are ways the fields may converge. More information than ever is available, and online stores allow anyone to buy GRIN technology. Today even children use and experiment with biotechnology. These trends suggest that many advances in technology will take place outside government or academic laboratories. As such, it is vital that defense planners follow and understand these trends.

With little effort and minimal cost, individuals can get used biological laboratory equipment on eBay, whole-genome sequences in free databases, and biology toolkits that combine simple parts. Common goals and information are shared on well-established Web sites and in discussion groups across a diffuse network. However, such a light footprint makes it difficult to assess the intent of these amateur scientists. It is vital that defense planners follow and understand these trends.

At present, there is no more important scientific field than biology. There have been dramatic advances in predictive biology (information management, computational modeling, data mining), systems biology (modeling complex systems in silico), and synthetic biology (creating artificial biosystems de novo from basic building blocks). As a result, biological systems have never been better understood, manipulated, or engineered.

Much GRIN research is dual-use; identical findings can be used for malicious or benign purposes, depending on intent. For example, applied research on brain function, which may help patients with cranial maladies, may allow development of biological agents that cause amnesia, violence, or depression, which could be dangerous to soldiers and civilians. Biological agents are widely available and have many uses. Malicious research can be hidden in legitimate laboratories working on the effects of such agents. What is troubling is not that such agents can be created, but that technology might be combined with these advances in other areas.

Although most people engaged in such research are innocent, it is easy for a loner or small group to invade the benign circle and use the information in a harmful manner. The fields of robotics and information technology have been open to research communities for years. Some successful computer hacking attacks have been mounted by smart, motivated young individuals. At the same time, similar people with different motives

Continued on p. 66

The Use of Space in Global Communications

It took 6 months for President James Polk to send a message to the West in 1845. At the time, communications with the West Coast went by sea around the Horn of South America or by ship, train, and ship across the Isthmus of Panama. The Pony Express began service in 1860. Its first trip from Missouri to California took 10 days, 7 hours, and 45 minutes, with riders covering 250 miles a day. Delivering mail by horseback over prairies, plains, deserts, and mountains, it was the fastest service across the North American continent. The Pony Express reflected the need for a rapid and reliable transcontinental communications system that operated year round. After it was replaced by the telegraph, the Pony Express became a legend of the Old West.

Less than 100 years later, the first satellite was launched into orbit and transmitted radio communications from space. Today, there are more than 850 satellites (see figure 3–2) in orbit that connect practically every place on Earth, simultaneously in near real-time, providing worldwide services. In fact, satellite-based services pervade almost every aspect of daily life and enable the globalized economy. As Alvin and Heidi Toffler have observed, the networked economy has led to the greatest changes in the global economy since the Industrial Revolution.

Different ways of communicating and providing services via satellite are foundations for the new wealth created in the so-called third wave of economic development. Although fiber optic cables remain technologically dominant over satellite communications for fixed, point-to-point telecommunications, satellite communications are critical to the global economy as an adjunct. Satellite communications provide point-to-multipoint and regional telecommunications services that lack wired infrastructure. They also enable the conduct of military operations worldwide, particularly for missions in regions with limited wired infrastructure. Those telecommunications no longer move primarily over dedicated military satellite communications systems. During the opening phase of Operations Enduring Freedom and Iraqi Freedom, some 60 and 80 percent of communications were sent over commercial satellite systems, respectively.[1]

Moreover, satellite communications provide other services such as positioning, navigation, timing data, and high-resolution commercial imagery, and they contribute to global utilities. Highly accurate positioning and navigation data improve productivity while lowering time and costs of transportation around the world. This information has improved understanding of the world and created new industries and services. Likewise, accurate timing signals enable synchronization for digital compression techniques and provide time stamping to authenticate billions of dollars in the daily international flow of capital. In addition, the resolution, volume, and selection of visual and multispectral imagery in almost all areas underpin both free products such as Google Earth and tailored value-added products that combine data for specific applications. The information that these services provide to individuals is of better quality and more timely and accessible than what was available to the superpowers during the early days of the Cold

War. Cumulatively, these satellite-enabled services fuel global transparency and transform global politics.

The confluence of satellite-based services, information systems, and networks brings together people, ideas, and goods from around the world at an unprecedented rate. As the title of Thomas Friedman's book put it, "the world is flat." Or at least it is in the process of flattening, since "it is now possible for more people than ever to collaborate and compete in real time with more other people on more different types of work from more different places and on a more equal footing than at any previous time."[2] This flattening also means "that we are now connecting all the knowledge centers on the planet together into a single global network, which could usher in an amazing era of prosperity, innovation, and collaboration."[3] Although the world is flattened to a certain extent, some groups are largely disconnected, which creates dangers and opportunities, as Thomas Barnett has emphasized: "Disconnectedness allows bad actors to flourish by keeping entire societies detached from the global community and under their control."[4]

The appetite for information is almost insatiable and growing exponentially. It is stimulated by technological advances in information and communications technology. From 2002 to 2007, annual worldwide revenues earned by satellite industries grew at an average rate of 11.5 percent, fueled by satellite television and direct broadcasting. When comparing revenue by sector, satellite services have driven the entire industry, showing continued growth of 18 percent in this period.[5] As the demand for more capacity, enhanced reliability, and wider coverage by communications systems increases, it should be noted that this capacity, like other limited resources, is scarce and should be husbanded until the next technological leap. Space contributed more than $251 billion to the global economy in 2007 and supported a range of activities from credit card validation and fleet truck management to precision agriculture and high-speed Internet, cell phone packet switching, and television and radio distribution.

Space-based services also present the opportunity to address a pressing global issue: energy. The potential to harness the Sun as an endless source of energy through space-based solar power could be vital to future generations. The wealth generated by space-based services could become the fourth wave of economic development postulated by the Tofflers. Moreover, the U.S. role in human and robotic space exploration has expanded knowledge of the universe and may improve the ability to address other long-term challenges such as protecting the planet from collision with near-Earth objects. These challenges will require a stable and sustainable security environment as well as refined governance to encourage and facilitate cooperative solutions.

Probably the most compelling reasons for generating wealth from space-based services are changing demographics and exploding world population. The United Nations issued a report in 2007 predicting that the world population will grow by 2.5 billion in the next 43 years, from the current 6.7 billion to 9.2 billion in 2050. This single increase is the equivalent of the total world population in 1950. Moreover, this increase will be absorbed largely by less developed regions, whose population is projected to increase from 5.4 billion in 2007 to 7.9 billion in 2050.[6]

Space-based satellite services have profoundly affected global systems and shaped aspects of national and international power. This impact will increase as technological advances spur new applications and create more interdependencies in the globalized environment. Accordingly, the United States must be the global leader in space and in the delivery of space capabilities. It must use spacepower to enable all instruments of power to exercise national sovereignty in space and secure the space domain for legal purposes.

NOTES

[1] Ronald M. Sega, Under Secretary of the Air Force, Space Posture Statement to Strategic Forces Subcommittee of House Armed Services Committee, March 16, 2006, 9.

[2] Thomas L. Friedman, The World is Flat: A Brief History of the Twenty-first Century (New York: Farrar, Straus and Giroux, 2005), 8.

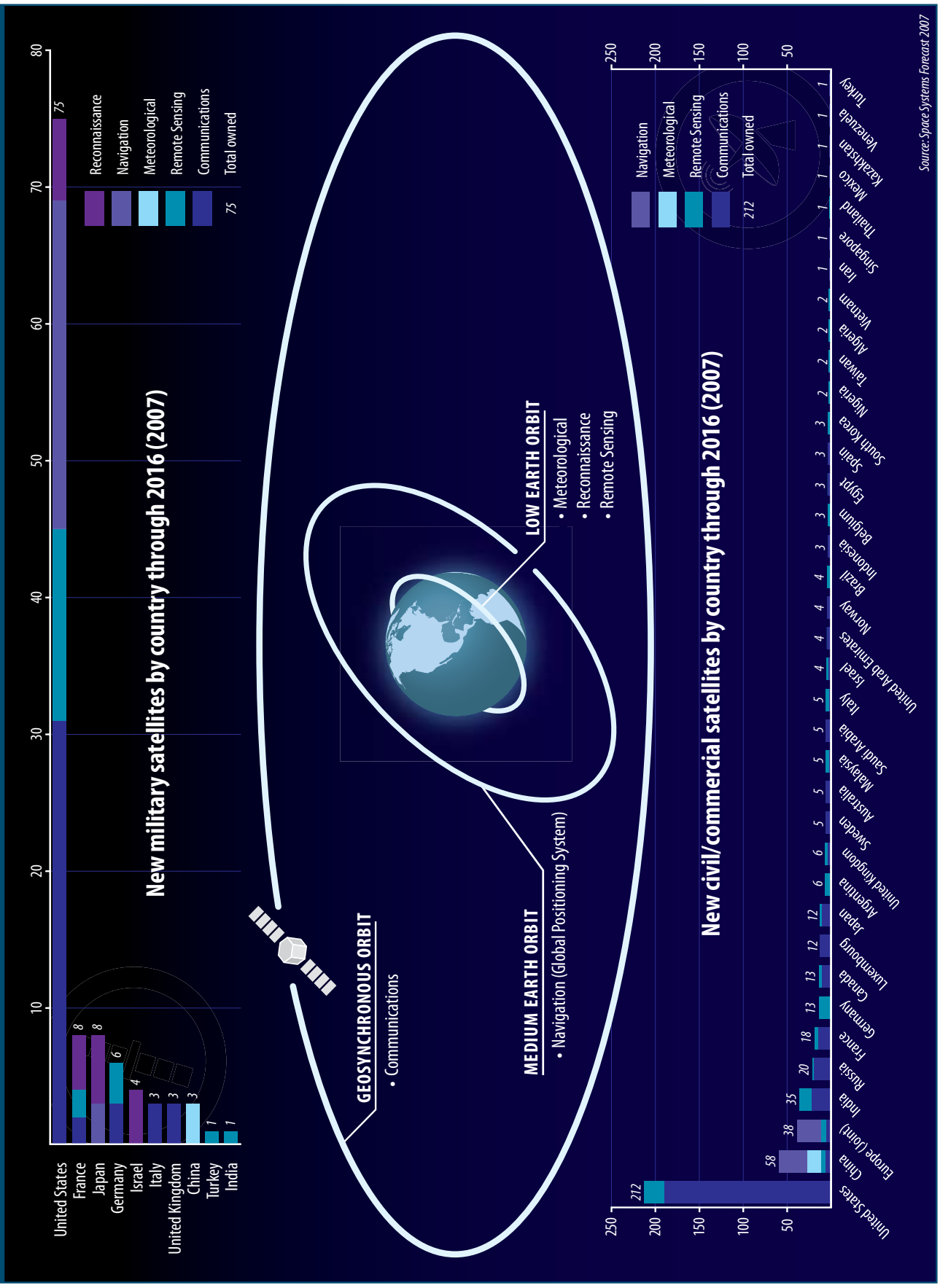
[3] Ibid.

[4] Thomas P.M. Barnett, The Pentagon's New Map: War and Peace in the Twenty-first Century (New York: G.P. Putnam's Sons, 2004), 8.

[5] State of the Satellite Industry Report, sponsored by the Satellite Industry Association, prepared by Futron Corporation, June 2008.

[6] Thomas L. Friedman, Hot, Flat and Crowded: Why We Need a Green Revolution—and How It Can Renew America (New York: Farrar, Straus and Giroux, 2008), 28.

Figure 3–2. Satellite Technology



Continued from p. 63

drove innovation at places such as Google. Amateur biologists and nanotechnology engineers are likely to do the same thing.

The defense implications go beyond biological threats. Dramatic performance enhancements would be a huge shock to warfare. Although large nations are likely to lead in the development of such enhancements, ruthless and unethical nations will have an advantage in this competition. GRIN research facilitates the modification of human beings for specific purposes. Initially, this manipulation was seen as a way of relieving illnesses such as tumors or discovering disease-causing genes. Now, however, it is also seen as a conduit to "improving" human beings.

There is substantial research being done on the posthuman future. Designer drugs produced in biotech labs interact with the brain in a genotype-specific manner either to improve memory or decrease the effects of sleep deprivation. Research on the brain-machine interface promises improvements in human senses such as hearing and vision. Exoskeleton suits allow soldiers to carry 200 pounds and bound long distances with little effort. Custom replacement organs will soon be generated from stem cells, and prosthetics with microprocessors will aid wounded soldiers.

Nanotechnology is a developing area, but it clearly links human biotechnology in various ways. A good deal of nanotechnology research is tied to biotechnology, which looks at the possible manipulation of the atom on the biomolecular level. It has even been posited that the robo-soldier of the future—rather than a human "cyborg"—may be a micro- or nano-robot that is versatile, inexpensive, impossible to detect, and able to penetrate nearly any space.

U.S. Navy (John F. Williams)

Marine monitors virtual scenarios from control room of Gruntworks Research for Infantry Integration Testing facility

While it is clear that the trends previously discussed are fairly well understood among the scientific community, they are not well understood in the defense or civilian arena. We must develop a "first principle" understanding of what drives these trends and a method to assess the impact of these inevitabilities. We must understand the disruptive consequences that may result from the intersection of these technological trends. Only then can we leverage these advances to create risk management strategies. A sense of where these trends are headed is also an essential component of a robust strategy, which enables us to plan for and prevent potential disasters.

What is fueling these trends? Computing power is a relatively free global commodity, the net effect of which is that the barriers to competition in many areas are falling. Consequently, the concept of a peer competitor is taking on new meaning for defense planners. No longer can potential adversaries be limited to nations with large gross domestic products and large military arsenals. One example of lower barriers to competition is found in the world of information technology. Cyberspace has evolved into the most important global commons. Access to cyberspace is essential for national security, military competitiveness, and economic prosperity, and unfettered access to information is key to national power. Various actors are competing for dominance in this new commons, including adversarial nations as well as individuals, terrorist groups, and criminal hacktivists.

The 20th century was dominated by weapons systems based on advances in physics, engineering, computing, and mathematics, colloquially known as *big bang, big metal*. The future presents a range of new threats and increasingly inventive biological weapons that can cripple major bodily functions even as the same bioengineering advances offer great potential for medical science.

But defense planners must remain aware of the malicious use of engineered biological agents in combination with robotics, information technology, or nanotechnology for two reasons. First, there is the potential for nonstate actors and nations to conduct ambiguous aggression or subtle war. Such aggression is a situation in which a bioattack causes a deadly outbreak but is not seen as such. Instead, the outbreak may be blamed on either an influenza

pandemic or abnormality in the food supply. This potential ambiguity makes defense planning and response highly complex. The second concern stems from the ease with which biological building blocks can be obtained. The widespread access to biological materials presents individual engineers with the capability to produce harmful agents that facilitate the creation of superempowered actors with the means to inflict large-scale global damage. The next generation of suicide bombers could be biobombers who infect themselves with bioengineered diseases and penetrate large population centers.

Nanotechnology is regarded as a major revolution in technology that enables structuring and restructuring of matter on a fundamental level. According to William Schneider, chair of the Defense Science Board, "Nanoscale sensors have the potential to dispel the fog of war. Richness in sensors allows commanders to have a complete picture of the tactical battlefield." Advances in nanotechnology could produce lighter, stronger, heat-resistant materials for new weaponry and make armor harder, camouflage better, military transport faster, and energy more efficient.

Nanotechnology is the key to distributed and configurable manufacturing, a model for goods produced locally near their point of use, which could have profound economic, social, and political impacts. Secure methods of obtaining electronic subcomponents are increasingly difficult in the globalized manufacturing economy. Distributed and configurable manufacturing could assure that production designs, manufacturing infrastructure, and even applications could be controlled securely.

There are significant advantages to manufacturing goods locally for defense, intelligence, and security applications rather than depending on a globally interconnected production chain. When manufacturing is done at the point of need, it is difficult to affect the national economy with a disaster or small number of attacks. The implications of local manufacturing might alter basic concepts of military operations, logistics, and sustainment. But strategically, planners must take account of the unintended consequences in destabilizing the interdependent globalized economy.

Defense planners have often anticipated new technologies to provide them with a competitive advantage, only to find their plans are flawed when viewed through the lens of moral principles. That debate continues today. In fact, some argue that the creation of autonomous soldier-robots with a conscience may be possible and that they may even be preferable to human soldiers.

Trends in ubiquitous computing, connectivity, and information-sharing will complicate future national security challenges. Some contend that this trend contributes to the decentralization or shift in power from nations to individuals or groups that are ill defined by political borders. The propagation of cutting-edge technologies that could harm national security interests are no longer reserved for elite, economically endowed nations. The result is much broader potential threats and increased uncertainty and ambiguity about the entities that may challenge the United States. This type of asymmetric attack, conducted by small groups in an ideological minority against a large group of potential victims, presents complex problems for defense planners.

Increased worldwide connectivity means people are more likely to encounter sympathetic co-conspirators, if only virtually. Social networks serve as recruiting mechanisms and offer added support for individuals who may want to launch such attacks. The social network of a potential attacker might create opportunities for simultaneous strikes across many locations.

New technologies are being developed at a fantastic pace and may intersect in unimaginable ways. Such advances potentially offer enormous benefits but create national security paradigms with challenges. Defense planners must be aware of the fact that new technology has unintended consequences as well as the potential for dangerous misuse in the hands of adversaries. **gsa**

NOTES

[1] GlobalSpec! offers a variety of products in response to the query "computer network attack." This is a good place to learn about network components, as opposed to attack tools, per se; see <www.globalspec.com/Industrial-Directory/Computer_Network_Attack>. Developer.net has a section on "measures of effectiveness" for computer network attack; see <www.developers.net/tsearch?searchkeys=measures+of+effectiveness+computer+network+attack>. There even are patent applications (for example, attack classification method for computer network security); see <www.freepatentsonline.com/y2008/0083034.htm>.

[2] See, for example, Hackers Home Page at <www.hackershomepage.com/>; How to Become a Hacker at <www.catb.org/~esr/faqs/hacker-howto.html?PHPSESSID=22f7378d0d1ea654962a22bf13166a5a>; and Secureroot at <www.secureroot.com/>.

[3] See also a range of attacks described by Ed Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, ed. Franklin D. Kramer and Stuart Starr (Washington, DC: National Defense University Press, 2009).

[4] "Satan" is a software program that claims to "identify weaknesses in just about any network connected to the Internet."

[5] See Dr. Mark Drapeau's informative posts about Government 2.0 at <www.mashable.com>.

[6] Evgeny Morozov, "An Army of Zeros and Ones: How I became a soldier in the Georgia-Russia cyberwar," available at <www.slate.com/id/2197514/>.

Contributors

Dr. Thomas X. Hammes (Chapter Editor) served 30 years in the U.S. Marine Corps, including duty in Somalia and Iraq. He holds a Masters of Historical Research and Ph.D. in Modern History from Oxford University and has lectured widely at U.S. and international staff and war colleges. He is the author of *The Sling and the Stone: On War in the 21st Century* (Zenith Press, 2004) and over 80 articles and opinion pieces.

Evan Applegate contributed graphics support this chapter. He received his B.A. in international relations with a concentration in peace and security from the University of California at Davis in 2009. He is head print designer for the Center for Biophotonics Science and Technology.

Dr. Mark D. Drapeau is Associate Research Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University (NDU). He has a B.S. and Ph.D. in biology from the University of Rochester and University of California, respectively.

Dr. Peter L. Hays is a Senior Scientist with the Science Applications International Corporation supporting the Policy and Strategy Division of the National Security Space Office in the Pentagon and also serves as an Associate Director of the Eisenhower Center for Space and Defense Studies at the U.S. Air Force Academy.

Lieutenant Colonel Robert Klingseisen, USA, is Deputy Chief for Policy and Strategy in the National Security Space Office. He is the former Chief, Space Operations Division, U.S. Strategic Command and Assistant Professor of Geospatial Sciences at the U.S. Military Academy.

Dr. Martin C. Libicki is a Senior Policy Researcher at the RAND Corporation. He has written extensively on cyberspace, most notably *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007).

Terry J. Pudas is a Senior Research Fellow in CTNSP at NDU. Prior to joining the center, he served as the Deputy Assistant Secretary of Defense (Acting), Forces Transformation and Resources, in the Office of the Under Secretary of Defense for Policy. In September of 2001, he was appointed as the Deputy Director of the newly created Secretary of Defense Force Transformation Office. He served as the Acting Director from January 2005 to October 2006.

Mark E. Stout is a Research Staff Member at the Institute for Defense Analyses. He is the lead author of *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movements* (Naval Institute Press, 2008).

Kim A. Taipale is the founder and Executive Director of the Center for Advanced Studies in Science and Technology Policy. He is also a Senior Fellow at the World Policy Institute and an adjunct professor of law at New York Law School.

Dr. Linton Wells II is a Distinguished Research Fellow in CTNSP at NDU, where he also serves as the Force Transformation Chair. Prior, he served in the Office of the Under Secretary of Defense (Policy) from 1991 to 1998, and finally as the Deputy Under Secretary of Defense (Policy Support).