Fourth Generation Warfare Evolves, FIFTH EMERGES

Colonel T. X. Hammes, USMC, Retired

SEVENTEEN YEARS AGO, a small group of authors introduced the concept of "Four Generations of War." Frankly, the concept did not get much traction for the first dozen years. Then came 9/11. Some of the fourth-generation warfare (4GW) proponents claimed that the Al-Qaeda attacks were a fulfillment of what they had predicted. However, most military thinkers, for a variety of reasons, continued to dismiss the 4GW concept. In fact, about the only place 4GW was carefully discussed was on an Al-Qaeda website. In January 2002, one 'Ubed al-Qurashi quoted extensively from two *Marine Corps Gazette* articles about 4GW.[1] He then stated, "The fourth generation of wars [has] already taken place and revealed the superiority of the theoretically weak side. In many instances, these wars have resulted in the defeat of ethnic states [*duwal qawmiyah*] at the hands of ethnic groups with no states."

Essentially, one of Al-Qaeda's leading strategists stated categorically that the group was using 4GW against the United States—and expected to win. Even this did not stimulate extensive discussion in the West, where the 9-11 attacks were seen as an anomaly, and the apparent rapid victories in Afghanistan and Iraq appeared to vindicate the Pentagon's vision of high-technology warfare. It was not until the Afghan and Iraqi insurgencies began growing and the continuing campaign against Al-Qaeda faltered that serious discussion of 4GW commenced in the United States.

Yet today, even within the small community of writers exploring 4GW, there remains a range of opinions on how to define the concept and what its implications are. This is a healthy process and essential to the development of a sound concept because 4GW, like all previous forms of war, continues to evolve even as discussions continue. That brings me to the purpose of this article: to widen the discussion on what forms 4GW may take and to offer a possible model for the next generation of war: 5GW.

Colonel Thomas X. Hammes, USMC, Retired, is a well-known writer and commentator on military affairs. He has a B.S. from the United States Naval Academy, an MSt from Oxford University, and is a graduate of the Marine Corps Command and Staff College and the Canadian National Defense College. In his thirty years in the Marine Corps, Colonel Hammes served at all levels in the operating forces and participated in stabilization operations in Somalia and Iraq. He is the author of The Sling and the Stone: On War in the 21st century *(Zenith Press, 2004), a much-discussed book on how to combat modern insurgency.*

Developments in 4GW

Current events suggest that there are a number of ongoing major developments in 4GW: a strategic shift, an organizational shift, and a shift in type of participants.

Strategic shift. Strategically, insurgent campaigns have shifted from military campaigns supported by information operations to strategic communications campaigns supported by guerrilla and terrorist operations. While there is no generally agreed upon definition of 4GW, according to the definition I wrote in 2003, "Fourth generation warfare uses all available networks—political, economic, social, and military—to convince the enemy's political decision makers that their strategic goals are either unachievable or too costly for the perceived benefit. It is an evolved form of insurgency." The key concept in this definition is that 4GW opponents will attempt to directly attack the minds of

enemy decision makers. The only medium that can change a person's mind is information. Therefore, information is the key element of any 4GW strategy. Effective insurgents build their plans around a strategic communications campaign designed to shift their enemy's view of the world.[2]

It is clear that many insurgent groups understand this fact. Hezbollah's strategy during the 2006 summer war with Israel is an excellent example. During the fighting, they focused not on damaging Israel, but on insuring they were perceived as defying the most powerful army in the Middle East. Thus, the fact that Hezbollah fired as many rockets on the last day of the war as the first was critically important. They know 122mm rockets are notoriously inaccurate and cause little damage, but the rockets are highly visible. Their appearance "proved" the powerful Israeli Air Force and Army had not hurt Hezbollah badly.

Once the fighting stopped, Hezbollah showed an even greater grasp of strategic communications. While the West was convening conferences to make promises about aid at some future time, Hezbollah representatives hit the streets with cash money and physical assistance. To the Arab world, the contrast could not have been clearer. When Israel needed more weapons, the United States rushed them in by the planeload. When Arab families needed shelter and food, we scheduled a conference for some future date. Hezbollah acted—and gained enormous prestige by doing so. To insure they continued to dominate this critical communications campaign, Hezbollah physically prevented other agencies from distributing aid in Hezbollah areas. The message was clear—Hezbollah was sovereign in its territory and focused on its people. The contrast between that message and the usual apathy of Arab governments to their people's needs was stunning.

Hezbollah is not an isolated case. The high quality and enormous variety of insurgent web sites indicate many, if not most, insurgent groups understand the imperative of executing an effective strategic communications campaign when trying to drive out an outside power. In contrast, the United States continues to flounder in its efforts at strategic communications.

This shift from Mao's three-phased insurgency to a strategic communications campaign has been developing since Ho Chi Minh's successful effort at breaking America's political will over Vietnam. Today, it is clearly the primary choice of insurgents faced with outside powers. However, just as Mao's strategic concept included a Phase III conventional battle to defeat the government, the new "coalitions of the willing" know they will also face a final phase. Theirs will be the civil war to decide who among them will control the country after the outside power is gone. Unfortunately, post-Soviet Afghanistan and today's Gaza Strip show that once the outside power is driven out, the civil war quickly devolves from 4GW to a traditional 2GW war of attrition.

Organizational shift. The emergence of civil war as a part of insurgency is based on the major organizational shift that has occurred since Mao formulated his concept. It reflects the continuous, worldwide shift from hierarchical to networked organizations. While the Chinese and Vietnamese

AFP, Denis Sinyakov

An Israeli fireman examines fires caused by Katyusha-style rockets fired by Hezbollah from southern Lebanon into the northern Israeli border town of Kiryat Shmona, 9 August 2006. Terrified and exhausted residents of the city fled from the daily rain of Hezbollah rockets in the first evacuation of an entire town since the creation of Israel.

insurgencies were hierarchies that reflected both the social organizations of those societies and the dominant business and military organizations of the time, recent insurgencies have been networked coalitions of the willing. For instance, in Iraq, there is no unifying concept among the various insurgent groups except to get Americans out of the country. While some of the more centrist groups could form a coalition government, clearly the Sunni Salafists and Shia religious militias cannot coexist if we are driven out; in fact, they are already fighting a civil war in anticipation of our departure. Other groups, such as criminal networks, cannot tolerate a strong central government of any kind–unless it is thoroughly corrupt and lets them continue their criminal activities.

The rise of networked coalitions is in keeping with the fact that both the societies in conflict and the dominant business organizations of our time are networks. Like society as a whole, insurgencies have become networked, transnational, and even trans-dimensional. Going beyond simple real-world networks, some elements of their organizations exist in the real world, some in cyberspace, and some in both dimensions.

Shift in participants. As part of the organizational shift, we have seen a change in who is fighting and why. It is essential for us to understand that, even within a single country, the highly diverse armed groups that make up a modern insurgency have widely differing motivations. Studying the motivation of a group gives us a strong indication of how that group will fight and what limits, if any, it will impose on its use of force. The UN's *Manual for Humanitarian Negotiations with Armed Groups* states, "In terms of founding motivations, armed groups generally fall into three categories: they can be *reactionary* (reacting to some situation or something that members of the groups experienced or with which they identify); they can be *opportunistic*, meaning that they seized on a political or economic opportunity to enhance their own power or positions; or they are founded to further *ideological* objectives."[3]

Like society as a whole, insurgencies have become networked, transnational and even trans-dimensional.

Reactionary groups often form when communities feel threatened. They tend to be sub-national or national groups that operate in specific geographic areas and attempt to protect the people of those areas. In essence, these armed groups represent a return to earlier security arrangements; they are the result of a state's failure to fulfill its basic social contract of providing security for its population. The ethnic-sectarian militias we have seen develop around the world in response to insecurity are reactionary groups. The Tamil Tigers and Badr Militia are typical of the type.

Reactionary groups need to protect populations but lack the military power to do so. As a result, they usually resort to 4GW–but generally use only conventional arms. While highly effective, such weapons are familiar to Western armies and thus easier to anticipate and defeat. Reactionary groups also tend not to be a threat outside their areas since they are focused mainly on defending their own people. However, they still conduct sophisticated communication campaigns to defeat outside powers.

Opportunistic groups spring up to take advantage of a vacuum to seize power or wealth. Criminal by nature, these groups have been around for centuries. What is different now is that commercially available weapons allow them to overmatch all but the most well-armed police—they are even a match for the armed forces of some nations. Opportunistic groups include organizations like Mara Salvatrucha 13 (MS-13) and, increasingly, the Irish Republican Army (IRA). Opportunistic groups conduct their own strategic communications campaigns, usually citing a religious or national cause to claim legitimacy for their criminal activities.

A third great motivator, *ideology*, gives birth to the most dangerous armed groups—organizations like Al-Qaeda, Aryan Brotherhood, and Aum Shinrikyo. Ideological groups are more dangerous to the United States than reactionary or opportunistic groups because of their no-limits approach to conflict. In the past, they have used society's assets against it. From Timothy McVeigh's bomb made of fertilizer and diesel fuel to Al-Qaeda's employment of airliners, ideological groups tend to be highly creative in their attacks. They are more likely to use society's infrastructure—chemical plants, mass

shipments of fertilizer, even biotechnology—as weapons of mass destruction than groups motivated by self-defense or opportunism.

Of even more concern is the fact that ideological groups are essentially impossible to deter. First, their "cause" provides moral justification, and sometimes a moral requirement, to use any available weapon. Second, they have no return address, so they do not fear massive retaliation—If Al-Qaeda detonates a nuclear device on U.S. soil, where exactly do we fire our nukes in return?

Ideological groups will not be deterred even by the danger inherent in the use of biological weapons. While other groups may hesitate to release a contagious biological agent for fear of killing their own people, ideological groups believe the higher power guiding their actions will either protect their members or call them home for their earned reward. Thus, the combination of extraordinarily rapid advances in biotechnology and the spread of ideologically driven armed groups represents a major threat to the global population.

While the UN manual cites three kinds of differently motivated insurgent groups, recent developments point to the advent of a fourth: a hybrid spurred by a blend of reactionary, ideological, and/or opportunistic motivations. Sometimes these groups are reactionary or ideological, but then turn to crime for funding. Al-Qaeda, for instance, is primarily an ideological group that has become increasingly opportunistic in order to subsidize its operations. The IRA started as a reactionary group, but it too has increasingly turned to crime—and may actually have moved from a reactionary to a purely opportunistic motivation.

Another kind of hybrid is the ideological group that finds itself de facto ruler of an area: by taking charge, it becomes bound to protect the community, just as reactionary groups must. The Jaysh Al Mahdi militia in Iraq is one such example.

Some groups can even fall into all three categories. For instance, Hamas and Hezbollah provide protection, espouse an ideology, and participate in crime for funding. In fact, most armed groups now use crime to fund operations.

The sad truth is that there is a truly alarming variety of armed groups active in the world today. Understanding their motivations, methods, and goals is becoming increasingly difficult.

Weapons of Mass Destruction

Iraq has seen the development of another major refinement of 4GW: using more or less basic materials to create weapons of mass destruction (WMD). While Western intelligence agencies have long worried that the Iraqi insurgents would use industrial chemicals, only recently have they used chlorine as part of their attacks. Much like World War One's combatants, the insurgents had to learn that it takes the right conditions and huge quantities of gas to create large numbers of casualties; however, they and their brethren around the world have shown a distinct ability to learn from each other, and now the Iraqi attacks are becoming increasingly effective. Although it might be nearly impossible to repeat, Al-Qaeda's 9/11 operation with airliners was certainly a massively destructive attack forged from unconventional (nonnuclear, non-chemical, non-biological) WMD materials. In contrast to 9/11, the extensive availability of toxic industrial chemicals means that massive chemical attacks can be duplicated in many areas of the world.

What makes this WMD-like development particularly troubling is that some terrorist websites have discussed using chemical plants or shipments to cause the numbers of casualties that occurred, for instance, in Bhopal, India, in 1984, when fumes from an industrial gas leak enveloped the city, killing thousands. The 1947 disaster in Texas City, Texas, when a ship with 8,500 tons of ammonium nitrate on board blew up in port and killed nearly 600, is another possible template for achieving WMD-like effects. If either incident had been intentional, it would have qualified as a WMD attack. This move toward unconventional WMD development, coupled with the trend shown by the Iraqi insurgents' increasingly effective use of chlorine, presents an immediate and major danger to U.S. interests both at home and overseas.

Another New Player: Private Military Companies

A largely overlooked development in warfare is the exceptional increase in the use of private military companies (PMCs). These organizations have always been around, but during the last two decades they have become central to the way the United States wages war. There has been very little consideration given to how PMCs might impact

A locomotive and debris after the 1947 Texas City Disaster.
Reprint, with permission, from Moore Memorial Public Library, Texas City, Texas.

international relations in general and war in particular. While we have focused on the monetary and political cost-cutting benefits of PMCs, other nations are discovering creative ways to use them to avoid normal international constraints on the use of force.

Of particular concern is the use of armed contractors. The length of this article prevents a full exploration of the numerous implications that flow from the increased use of armed contractors, so I will simply offer some thoughts to start a discussion. For instance, How does one hold a country accountable for the actions of an armed PMC? How will these companies change the face of armed conflict? What impact will they have on the relationship between the rulers of resource-rich countries and their populations? Can they be employed to provide bases or major forward-deployed combat assets?

PMC spokesmen have continually reassured us that their companies are responsible organizations that are working with governments to devise effective regulations for PMC employment. This is, in fact, true. However, while the United States has moved to increase the accountability of such companies through regulations and contracts, these methods have yet to be seriously tested. Further, much like the shipping industry avoids regulation by registering under flags of convenience, we can expect PMCs to do the same: if regulations interfere with how they wish to operate, they will move to another country or even dissolve their corporations and start again as different legal entities in different countries. We have already seen a number of PMCs do exactly that.

The sudden presence of PMCs in numerous conflicts worldwide presents some interesting challenges to the international community. In the more than 300 years since the Treaty of Westphalia, we have developed diplomatic, economic, and military techniques for dealing with crises created when nation-states use armed force—or even threaten to use it. We do not have such mechanisms in place when nation-states or even private individuals employ armed contractors. If China had announced that it planned to send multiple field armies to Angola to assist with security and construction there, the UN would at least have opened up a dialogue. Yet a Chinese company has signed a contract to do just that, except that it will substitute 850,000 armed and unarmed contractors for the field armies. This event has simply not shown up in international discussion. It is particularly interesting because China has just signed a 10-year contract with Angola to purchase oil at $60 a barrel. While the contractors are not an official branch of the Chinese Government, their presence clearly puts China in position to "resolve" any disputes with the Angolan Government over that contract. Thus, thanks to the creative use of PMCs, brokering agreements between nation-states and even the process of intervening to resolve disputes between parties has moved outside the international system. How does the UN respond to a contract dispute between an armed private company and a government?

Another interesting development is that "governments" of countries with resource-rich areas can employ PMCs to seize and hold the rich areas while they ignore the rest of the country. We have already seen this with local militias and "blood diamonds," but have not seen it applied in a systematic way. That may be happening now in the Sudan, where the Sudanese Government has hired Chinese firms to secure Sudan's oil facilities. These firms not only provide reliable security, but also have no qualms about how the Sudanese Government chooses to conduct its internal affairs. By using PMCs, a very small minority can control a country without any regard to the needs of the majority. A clique can always seize power through a coup, but it takes trusted security forces to keep the resulting governments in power. In some parts of the world, security forces are likely to be loyal to their own clans or tribes, so the government must take care of those tribes. Now, though, governments have the option of hiring an effective PMC and completely ignoring any parts of the country that are not profitable—they

won't need the people to insure their continued rule. The result will be a significant increase in the ungoverned and desperately poor areas of the world. Also reinforcing the power of an oppressive minority is the international community's policy of dealing with whatever gang controls a country's capital city. With little likelihood of outside intervention, the oppressed and poor will have to resort to violence.

PMCs can also be used to establish forward operating bases or can even be deployed as forward forces. In the same way the British used the East India Company to establish a navy, an army, and supporting bases in India, other nations such as China are using commercial entities throughout the world to protect or advance their interests. Chinese PMCs already constitute a major ground presence in Africa, and with Chinese commercial entities building ports all along the shipping lanes from the Middle East to China, China could employ naval PMCs, at least nominally, to provide security against pirates. In fact, in early March the Chinese signed a contract with Somalia to train and equip a Somali coast guard. Such naval forces will obviously need maintenance and support facilities, which the companies will build. In effect, China's PMCs can establish a chain of naval facilities complete with ships near the chokepoints of major sea routes.

PMCs cannot be easily categorized as belonging to a particular generation of war. Rather, they are a tool that can be used in a wide variety of ways. But because 4GW succeeds by avoiding an opponent's military strength, PMCs offer the intriguing possibility of a weak country employing them in a 4GW manner, so that war doesn't look like war, but like business.

The final alarming fact about PMCs is that they are *businesses*. As such, they compete by focusing on quality, reliability, and cost. China can match Western firms on the first two and, based on a huge population of unemployed young men, can severely undercut Western firms on cost. Further, China has a huge incentive to subsidize businesses like PMCs: its one child policy has resulted in over 20 million more Chinese men of marriageable age than Chinese women.

Criminals are yet another player in 4GW. Most 4GW discussions still focus on politically motivated insurgent groups, however, as discussed in the 1989 *Gazette* article on 4GW, criminal organizations are using 4GW techniques. A good example is Mara Salvatrucha 13 (MS-13). This organization started out primarily as a criminal movement, but it is now establishing effective political control in widely scattered locations. From some communities in El Salvador and Honduras to neighborhoods in American cities and even some American suburbs, MS-13 is creating sovereignty in non-contiguous territory. Much like their commercial predecessors the Hanseatic League, MS-13 has used violence and wealth generated by trade (primarily drugs) to create enclaves within national territories.

State Use of 4GW

China's employment of PMCs is a clear example of a state using 4GW. Iran has taken a very different approach. Last summer, it introduced the West to the concept of lateral asymmetric escalation. As the United States continued to raise the pressure for UN action in response to Iran's nuclear program, Iran seized the opportunity presented by the Israel-Hezbollah confrontation in Lebanon to change the discussion. While we do not think that Iran instigated the war, we know it has considerable influence over Hezbollah and certainly provided extensive support to that group's efforts against the Israelis. In Hezbollah, Israel faced a 4GW enemy that made effective use of relatively high-technology weapons to challenge Israel's assumed military superiority. External to Lebanon, Iran cooperated with Syria to provide extensive logistical and perhaps intelligence support to the Hezbollah command. Because the United States and UN apparently can deal with only one crisis at a time, Iran was able to use the conflict in Lebanon in a 4GW manner to stop action against its nuclear program. Obviously, this was not a long-term solution for the Iranians, but it furthered their apparent strategic goal of buying time to develop a nuclear weapon.

4GW Updated

Since the 1989 *Gazette* article, the Afghan and Iraqi insurgents have continued to shift their strategic focus to the 4GW aspect of strategic communications. Organizationally, the insurgents are evolving into an ever-increasing variety of armed groups linked into coalitions of the willing. Also, the types of players and their motivations have changed significantly over time.

As a result, the coalitions of the willing we are facing in Iraq and Afghanistan are much more challenging than their monolithic predecessors. The proliferation of motivations and merging of ideological, reactionary, and opportunistic groups makes it increasingly difficult to tell who is fighting and why. Fortunately, the bottom line remains effective security and governance for the people, and the new counterinsurgency field manual (FM 3-24, *Counterinsurgency*) provides solid guidance on how to achieve that. Unfortunately, the sheer number of people involved in the two conflicts precludes the United States from realizing the recommended ratio of one security officer to every 50 citizens that has generally meant success in the past. To deal with the numerous changes in 4GW, we will have to find new ways to provide security while building the political coalitions that are the only way to defeat an insurgency. We will also have to apply our diplomatic, economic, and political resources more broadly and effectively than we have done in the past to deal with the expanding nation-state use of 4GW.

Fifth Generation Warfare

"Military institutions and the manner in which they employ violence depended on the economic, social and political conditions of their respective states." —Clausewitz[4]

Like always, the old generations of war continue to exist even as new ones evolve. Today, we see grim 2GW firepower-attrition battles in parts of Africa even as the first hints of 5GW emerge. This should not be surprising—countries that lack the political, social, and economic systems to support new forms of war will continue to use the older forms. Yet a new generation must also evolve and, given the fact that 4GW has been the dominant form of warfare for over 50 years, it's time for 5GW to make an appearance. We should be able to get some idea of what this new form of war will be by examining how political, social, and economic systems have changed since 4GW became dominant.

To deal with the numerous changes in 4GW, we will have to find new ways to provide that essential security while building the political coalitions that are the only way to defeat an insurgency.

Politically, there have been major changes in who fights wars. The trend has been and continues to be downward from nation-states using huge, uniformed armies to small groups of like-minded people with no formal organization who simply choose to fight. We have slid so far away from national armies that often it is impossible to tell 4GW fighters from simple criminal elements. Many of the former are, in fact, criminal elements–either they use crime to support their cause or they use their cause to legitimize their crime.

Economically, we have seen a steady increase in the power of information. Insurgent groups have seized on the improving information grid to execute the strategic communications campaigns that are central to their victories. The content and delivery of information has accordingly shifted from the mass propaganda of Mao to highly tailored campaigns enabled by the new methods of communication and new social patterns. Insurgents have been quick to exploit such powerful communication tools as the cell phone and the Internet for recruiting, training, communicating, educating, and controlling new members. They have shifted from mass mobilization to targeted individual mobilization.

Today's key businesses are becoming ever more productive because of their access to or manipulation of information. One result has been a proliferation of small companies that have created great wealth, a phenomenon in accordance with the long-term trend of power devolving downward to smaller entities—whether they are business or military. The epitome of this tendency is that just two guys essentially created Google.

Communications is not the only burgeoning sector with implications for 5GW. Two industries with even greater potential to change our world—biotechnology and nanotechnology—are on the verge of huge growth.

In many ways military and business problems are merging as the world becomes more interconnected and power is driven downward. In 2006, a

group of about 20 angry Nigerians took hostages from a Shell oil platform in the Gulf of Guinea. Shell shut down its Nigerian Delta production and world oil prices rose dramatically. The interconnected world is highly vulnerable to disruptions in key commodities, and business issues can very rapidly become matters of serious international security. This is not the same as in the old banana wars, when Marines were consistently committed to protect American interests that mattered only to a few stockholders. Today, very small armed groups can impact the entire world's economy immediately and dramatically.

Socially, we have seen a major shift in how communities are formed. People are changing allegiance from nations to causes, a trend dramatically accelerated by Internet connectivity. In fact, many people are much more engaged in their online causes than in their real-world communities. Of particular concern are members of groups who are willing to go to extremes to advance their causes—from the woman who lived in a redwood for two years to suicide bombers. Such actors place their causes above any rational analysis of the impact of their actions—and they can be found through the Internet.

In sum, political, economic, and social trends point to the emergence of super-empowered individuals or small groups bound together by love for a cause rather than a nation. Employing emerging technology, they are able to generate destructive power that used to require the resources of a nation-state.

All of these new developments are of particular concern because emerging political, business, and social structures have consistently been more successful employing nascent technology than older, established organizations. Today, two emerging technologies, nanotechnology and biotechnology, have the power to alter our world, and warfare, even more fundamentally than information technology. Most writers agree it will be 20 years or more before nanotech hits full stride, so I will not discuss it further. In contrast, today's biotechnology can give small groups the kind of destructive power previously limited to superpowers.[5]

The October 2001 anthrax attack on Capitol Hill may have been the first 5GW attack. Given the enormous investigative effort expended on finding the perpetrator(s) and the fact that we have not made a single arrest, one has to believe the attack was executed by an individual or a very small group. Had more people had been involved, someone would have leaked information or been found.

If this is a valid assumption, then we had a super-empowered individual or small group attack the legislative body of a nation-state using an advanced biological weapon in support of an unknown cause. This individual or group disrupted the operation of Congress for several months, created hundreds of millions of dollars in clean-up costs, and imposed mail screening requirements (and associated costs) that are still in effect today—not a bad payoff for a few ounces of anthrax and some postage.

The anthrax attack provided stark evidence that today a single individual can attack a nation-state. Over time, the combination of political motivation, social organization, and economic development has given greater and greater destructive capability to smaller and smaller groups. While some technologists thought we had reached a peak of destructive power with the advent of thermonuclear weapons, the fact remains that creating and delivering such weapons required an elaborate and expensive developmental effort. By contrast, the following recent

EPA

Clean-up personnel use a HEPA vacuum in a congressional office after the anthrax incident on Capitol Hill in 2001.

developments suggest that the potentially massive destructive power of bio-weapons is within reach of motivated groups:

- Three years ago, a team led by Dr. Craig Venter created a functioning virus from off-the-shelf chemicals. Venter's team selected a specific virus, purchased the necessary genetic base pairs to make the virus, and then "assembled" the pairs into a functioning synthetic virus. All of the materials and equipment the team used are commercially available without restrictions. Venter has predicted that what took an elite team and a very well-equipped lab to do the first time could be done by any competent graduate student in a university lab in less than a decade.
- Paul Boutin, a science writer, decided to take up Venter's "challenge." Despite not having been in a biology lab since high school, Boutin, with a little guidance from Dr. Roger Brent to keep him out of dangerous experiments, created glowing yeast. While yeast is not smallpox, the equipment, techniques, and nucleotides Boutin used are similar to those needed to create smallpox from its base pairs.[6]
- The complete smallpox genome has been published online and is widely available. Boutin found it in about 15 minutes.
- The nucleotides to make smallpox can be purchased from a variety of suppliers without identity verification.
- Smallpox has about 200,000 base pairs. DNA with up to 300,000 base pairs has already been successfully synthesized.
- An Australian research team heated up mousepox virus by activating a single gene. The modification increased its lethality from 30 percent to over 80 percent. It is even lethal to 60 percent of an immunized population. They posted their result on the Internet. It turns out smallpox has the same gene.
- The cost of creating a virus is dropping exponentially. If Carlson's Curve continues to hold true, the cost of a base pair will drop to between 1 and 10 cents within the decade. Thus, a researcher could order all the necessary base pairs to create a smallpox virus for between $2,000 and $20,000.[7] The equipment he needs to assemble the virus will cost an additional $10,000.
- Bio-hackers are following in the footsteps of their info-hacker predecessors. They are setting up labs in their garages and creating products. Last year, a young British researcher invested $50K in equipment and produced two new biological products. He then sold his company, Agribiotics, for $22 million. We can assume hundreds, if not thousands, of young biology students are now in their basements attempting to make new biological products.

These discrete but related events mean that it is becoming increasingly easier for a small group and perhaps even an individual to create a virus such as smallpox and use it as a weapon.

Some experts have reassured us that even if a small group can create a biological virus, it is the testing, storage, and dissemination that are the most difficult steps in weaponizing a biological entity. They are right—if the creator uses traditional methods. However, a person can avoid the requirement for testing by selecting a known lethal agent, such as smallpox. He already knows it can thrive outside the laboratory. Storage and dissemination problems can be solved by tapping into the increasing trend of suicide attacks worldwide—he simply injects the smallpox directly into suicide volunteers, who become both the storage and the dissemination systems.

Using a few volunteers and commercial airlines, a terrorist group can create a near-simultaneous worldwide outbreak of smallpox. *Dark Winter*, an exercise conducted in 2001, simulated a smallpox attack on three U.S. cities. In a period of 13 days, smallpox spread to 25 states and 15 countries in several epidemiological waves, after which one-third of the hundreds of thousands of Americans who contracted the disease died. It was estimated that a fourth generation of the disease would leave 3 million infected and 1 million dead. The exercise was terminated at that time.[8]

It is essential to remember that not only will smallpox cause an exceptional number of deaths, but it will also shut down world trade until the epidemic is controlled or burns itself out. Given that the 2002 West Coast longshoreman's strike cost the U.S. economy $1 billion per day, the cost of a complete shutdown of all transportation will be catastrophic.

Biological weapons have the capability to kill many more people than a nuclear attack. Further, unlike nuclear weapons, which are both difficult and relatively expensive to build, smallpox will soon be both inexpensive to produce and difficult to detect until released. While I selected smallpox for this

brief paper, a biologist can obviously select any of the known effective contagions. He can also attempt to create an entirely new disease. But of course no one can predict how a lab-raised disease will fare against the natural enemies it will face when released into the environment. Thus, a terrorist is more likely to use an existing disease or modify one to be more lethal. He can also release both versions of the disease—the naturally occurring virus and the enhanced virus—to insure success.

Summary

Drawing on changes in the political, economic, social, and technical fields, 1GW culminated in the massed-manpower armies of the Napoleonic era. In the same way, 2GW used the evolution to an industrial society to make firepower the dominant form of war. Next, 3GW took advantage of the political, economic, and social shifts from an industrial to a mechanical era to make mechanized warfare dominant. Fourth-generation warfare uses all the shifts from a mechanical to an information/electronic society to maximize the power of insurgency. It continues to evolve along with our society as a whole, thus making 4GW increasingly dangerous and difficult for Western nations to deal with.

Fifth-generation warfare will result from the continued shift of political and social loyalties to causes rather than nations. It will be marked by the increasing power of smaller and smaller entities and the explosion of biotechnology. 5GW will truly be a nets-and-jets war: networks will distribute the key information, provide a source for the necessary equipment and material, and constitute a field from which to recruit volunteers; the jets will provide for worldwide, inexpensive, effective dissemination of the weapons.

The contagion scenario I described above is among the more devastating possible, but smallpox is only one weapon a super-empowered small group could use to attack society. They may use any number of evolving technologies. The key fact to remember is that changes in the political, economic, social, and technical spheres are making it possible for a small group bound together by a cause to use new technologies to challenge nation-states. We cannot roll back those changes, nor can we prevent the evolution of war. Clearly, we as a Nation, and particularly our military, are not ready to counter the coming attacks. It's time to start thinking about how we might deal with this next step in warfare. ***MR***

Fifth-generation warfare will result from the continued shift of political and social loyalties to causes rather than nations. It will be marked by the increasing power of smaller and smaller entities and the explosion of biotechnology.

NOTES

1. See William S. Lind, et al, "The Changing Face of War Into the Fourth Generation, "*Marine Corps Gazette*, October 1989. See also Thomas X. Hammes, "The Evolution of War: The Fourth Generation," *Marine Corps Gazette*, September 1994.

2. I have intentionally chosen to use "strategic communications campaign" instead of "information campaign" for two reasons. First, the Pentagon's definition of information operations states that "the principal goal is to achieve and maintain information superiority for the US and its allies." Unfortunately, it sees information primarily as computer and communications security and exploitation. Second, the very phrase "information operations" leads one to focus on the tactical or operational level. In contrast, "strategic communications" by definition falls at the strategic level of war and subsequent operational and tactical efforts must support that strategic approach.

3. United Nations *Manual for Humanitarian Negotiations with Armed Groups,* 16.

4. Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton UP, 1989), 6.

5. There has already been extensive discussion about cyber attacks, so I will not deal with that threat in this short article. However, such attacks are an option for small groups—to include the physical destruction of key fiber-optic switches and cables using simple breaking-and entering-techniques.

6. "Biowar for Dummies," <http://paulboutin.weblogger.com/stories/storyReader$1439>.

7. Robert Carlson, "The Pace and Proliferation of Biological Technologies," Biosecurity and Bioterrorism: BioDefense Strategy, Practice and Science, Volume 1, Issue 3, 2003.

8. Mark Mientka, "Dark Winter Teaches Bio Lessons," <www.usmedicine.com/article.cfm?articleID=322&issueID=33>.