
FOREWORD

Andrew W. Marshall

This effort to assess how the role of information in warfare is changing seeks to understand many of the remarkable developments under way in information and communications technology, and their potential effects on warfare. It is because the uncertainties are so substantial in this realm that this effort by Zalmay Khalilzad, John White, and their collaborators is so admirable. They are attempting to deal with a topic whose complexities and lack of consensus, at present, easily match its importance. The principal value in such an effort is that it helps to organize our thoughts and to sort out the areas of agreement and disagreement. Indeed, this volume reveals several important lessons that can be gleaned from the very different and distinct perspectives contained in it:

- Information advances will affect more than just how we fight wars. The nature and purpose of war itself may change. How wars start, how they end, their length, and the nature of the participants may change as shifts in the relative power of states and nonstate entities occur.
- New technologies cut both ways in terms of their effects on national security. Together, the chapters make clear that advances create new vulnerabilities; new threats create new opportunities. We should resist the temptation to see the changes documented here either as wholly bad or wholly good. Rather, we need to understand that profound technological changes are inevitably two sided.
- The Department of Defense (DoD) has little control over the pace and direction of the information revolution. Although in

the past DoD played an important role in developing, refining, and implementing new information technologies, today the technological envelope is being pushed largely by the commercial sector. DoD needs to manage a difficult transition from being a pioneer to being a leading user. This transition will require not only keeping abreast of new technological developments but also accepting that technology will no longer be developed exactly to military specifications.

- The increasing capacity to produce, communicate, and use information will have an important effect on every area of national security. Information is everywhere. As a result, we will not be able to understand how these new technologies will change our own jobs unless we understand how they will change the jobs of others. The advent of the information age will require, as never before, that we take a wider perspective and avoid stovepipes that blind us to changes taking place outside our own spheres of direct responsibility.

Considering how the U.S. defense establishment operates today, these lessons are important and not as self-evident as they might first appear. Unfortunately, they provide only the broadest guidance for how to adapt to the whirl of changes we face. As the chapters indicate, any consensus on more detailed instruction escapes us at the moment. In part, this is because changes at the level of information and information systems represent a particular challenge for understanding the future. In a recent work, Robert Axelrod and Michael Cohen provided some relevant insights into the particular complex uncertainties that we face.¹ Axelrod and Cohen refer to systems as “complex” not merely because they are being influenced by many simultaneous factors but also because of how those factors interact with each other.

[T]here are many systems with lots of moving parts that are nonetheless quite easy to predict—think of the gigantic number of colliding molecules in a perfect gas. By “complexity” we want to indicate something else: that the system consists of many parts

¹See Michael Cohen and Robert Axelrod, “Complexity and Adaptation in Community Information Systems: Implications for Design,” in Toru Ishida, ed., *Community Computing and Support Systems*, Heidelberg: Springer Verlag, 1998.

and/or processes each of which interacts significantly, and perhaps nonlinearly, with some of the others. Ecologies and brains seem to be well described as systems that are complex in this more socialized sense.

What makes prediction especially difficult in these settings is that the forces shaping the future do not act additively, but rather their effects are via nonlinear interactions among systems components. In such worlds events change the probabilities of other events—sometimes dramatically.

Warfare has always been nonlinear and complex in the sense that Axelrod and Cohen describe. Minor events have often produced disproportionate effects on an organization that consists of badly understood machines and unpredictable humans operating in an extraordinarily stressful environment. Despite this continuity, a profound and new message about complexity permeates this volume. As the sensors, networks, and communications systems both allow more information to be obtained about the battlefield, or the surrounding context of military action, and allow the coordination of the actions of separate military platforms and military units, military organizations have become ever more finely balanced on the edge of chaos.

It is very difficult to understand what happens to the functioning of these organizations when parts of these networks or parts of the overall system are disrupted in their functioning or possibly are destroyed. For the moment we do not have an analytic framework to get at such issues, and we certainly do not have adequate models. So the effects of changes in information levels or asymmetries or the effects of information warfare on the performance of military organization are matters of considerable uncertainty.

There is a second set of relevant problems that Axelrod and Cohen also surface. To illustrate the difficulty in foreseeing how the current information revolution may affect international politics, they look at a previous information revolution, namely the printing revolution:

[T]he printing revolution led in Europe to indirect effects that were often quite different from the immediate effects. Ancient authority was undermined even though good editions of ancient texts became accessible, scientific progress was promoted even though

pseudo-science was popular, religious divisions occurred even though information could be more widely shared, and national languages and states developed even though long range communication was fostered. All this should leave us humble about predicting the effect of the current Information Revolution. We can begin to see some of the direct effects, but we need to be aware that the indirect effects might be quite different and much more powerful.

With that as background, let me make some comments on two major issues that arise in nearly all of the chapters. First, as many of the contributions to this volume suggest, there are major vulnerabilities in the computer networks and in the information infrastructures of the United States, our military information systems, and undoubtedly other countries' military establishments. Some analysts have seen in these vulnerabilities new possibilities for strategic attack, launched from almost anywhere in the world, on the economy, national infrastructure, and military preparedness of a state.

History teaches us, however, that the immediate effect is often quite different and generally less important than the indirect effects. Every action creates a reaction; every new weapon spurs the creation of a new defense. The important question, therefore, is what the situation is likely to be 10 or 20 years from now. Will these vulnerabilities persist? Will the attackers keep ahead of the development of defenses?

Experience indicates that the current vulnerabilities may not persist. Little attention has been paid to building defenses until now. The technology is changing rapidly, and information systems continue to evolve as they keep up with these changes. Installing new systems every couple of years takes a lot of energy and attention. In some areas, especially in commercial domains where the interest is high and where the risks are seen more clearly, there has been a greater response to the threat of external intrusions. Certainly, the demand for the services of those who make a business of helping companies defend themselves is increasing at a very rapid rate. I am not in a position to judge how effective these protections are in the best cases, but I believe it is wrong to judge the future by our current state of vulnerability.

Similarly, there is a lot of speculation that the state will weaken as new media and cheaper means of communication empower smaller

groups. While this may be true, the more important question is how much and how fast? Roger D. Masters, a political philosopher at Dartmouth College, has pointed out that Machiavelli foresaw that the rise of the nation-state was inevitable in the early part of the 16th century.² Nonetheless, it took 200 years for the nation-state to emerge in something like its current form. Perhaps the state is in decline—given its current preeminence, its most likely direction is certainly downward. The real question is how long will it take? Will it decline faster than it ascended?

If one looks more narrowly at warfare in a theater, one can bring similar observations to bear about the uncertainty of change within complex systems. At this level of warfare, new information technologies are having an effect on almost everything from training to logistics to public relations. Not only will developments of new sensors, communications, and the capacity to process information allow new levels of coordination of dispersed, widely separated units, but almost all weapon systems will have new capabilities derived from the embedded microprocessors within them. Weapons and platforms are becoming smarter, and more decisions are being delegated to them.

As the result of such changes, forecasting in this realm is also laced with uncertainty. Nonetheless, two observations have emerged, both from this volume and from war games that my office has been conducting on warfare in 2020. First, long-range precision strike weapons coupled to systems of sensors and to command and control systems will fairly soon come to dominate much of warfare. The critical operational tasks will be destroying or disabling elements of an opponent's forces and supporting systems at a distance. Defeat will occur due to disintegration of command and control capacities, rather than due to attrition or annihilation.

Second, the information "dimension" increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one's own information systems and being able to degrade, destroy, or disrupt the functioning of the opponent's information systems will become a major focus of

²Personal communication.

the operational art. Obtaining early superiority in the information realm will become central to success in future warfare. It has always been important; it will soon be central.

In essence, however, these are predictions about where the action will be, not about how it will come out. Information and its associated technologies are destined to become a central focus on the battlefield. Does that mean that the offense or the defense will dominate? Will these developments favor states or terrorists? Will war become an exercise in media spin? In the face of the uncertainties of the future, and the disagreements of the present, I can only suggest caution and humility in predicting the future.