

17 Cyberwarfare and Cyberterrorism: Implications for Defense R&D

Peter A. Wilson

This chapter addresses cyberwarfare and cyberterrorism. To discuss this issue right now is like discussing the significance of air power, not in the 1920s or 1930s, but around 1910. We have not had any experience with cyberwarfare. This is a very new technology and not surprisingly there are some strong differences of opinion about its significance.*

RAND has explored the issues of information warfare and information operations for about five years. We have been engaged in a wide array of exercises known as the “Day After” series. We studied post-Cold War strategic warfare through policy planning gaming and the impact of the information revolution on warfare. These exercises are designed to put senior policymakers into a plausible future and present them with an uncomfortable scenario with the philosophy that the prospect of an execution helps concentrate the mind. It has been a successful tool to stimulate thinking about what we should do proactively before a crisis. Initially, these led to the U.S. Critical Infrastructure Protection (CIP) Exercises in 1995 and 1996. We also co-designed a number of foreign CIP exercises, and CIP contingency exercises for the Office of the Secretary of Defense (OSD).

Also, RAND has conducted extensive “Day After” exercises for the Department of Treasury’s Financial Crimes Enforcement Network (FinCEN). One of the interesting aspects of the emergence of the E-commerce world, or the E-world in general, is the prospect of new

Peter A. Wilson is a senior policy analyst at RAND. This article is based on remarks delivered at the 26th Annual AAAS Colloquium on Science and Technology Policy, held May 3–4, 2001, in Washington, DC.

opportunities for organized crime to profit from this technology. This critical area needs to be addressed in more depth.

One of the recurring themes in this field is that the information technology revolution is blurring the conventional institutional and bureaucratic boundaries between domestic and foreign, between crime and war, and between peace and conflict. This obviously raises very troubling tensions and uncertainties between national security, law enforcement and intelligence bureaucracies, which heretofore thought they knew their mission and their turf. Information technology is disturbing these relationships quite profoundly, especially in Washington, while also bringing about many positive transformations in our economy and in our society.

Critical Infrastructure Protection

Critical infrastructure protection (CIP) is the central notion that you are contemplating the possibility that opponents will take advantage of the information technology environment. The potential threats through the global information infrastructure (GII) or “cyberspace” are strategic warfare against critical infrastructures and terrorism against individual infrastructures. Traditionally, we have been concerned with physical sabotage, trans-oceanic nuclear war operations, and supporting U.S. expeditionary forces abroad. We were focused on physical attack. But things are different now. What is new about the CIP problem? There are several issues. One is the possibility of computer network attacks (CNA). Our ability to access data and/or interfere with networks has collapsed within cyberspace. We have seen an emerging revolution in how we can conduct business, crime, and war in cyberspace, which is, after all, a completely human created medium.

Another issue is computer network exploitation (CNE); that is, intelligence gathering for both national and private interests. One of the questions likely to emerge over time in a public policy and legal sense is what are the boundaries of computer network exploitation, or what constitutes an act of computer network attack. Naturally we will have our own or national perception of this, but potential international victims of computer network exploitation may interpret it in a very different way.

These concerns lead us to the need for a computer network defense (CND) against both strategic political military attacks and terrorist attacks. Strategic attacks are directed at the national critical infrastructures such as the telecommunications system, the IT technologies and

their infrastructures, financial networks, the networks that manage energy system, and transportation. Attacks through cyberspace would come most likely in conjunction with physical attacks. Cyberweapon techniques would be used to accelerate or further disrupt the ability of the first responders to react to physical forms of terrorism and/or strategic attacks.

We can see that IT related CIP concerns are much greater than the traditional homeland concerns. One of the key concerns, and a new one, is the synergy between cyber and physical attack.

Information Operations

Information operations (IO) have traditionally been an important element of tactical and operational warfare. But they have been a more modest element of strategic warfare. Offensive IO include not only electronic warfare (computer network attack and exploitation) but also psychological (perception management) operations. Defensive IO include computer network defense, information assurance, and operational security. Information assurance can be a very narrowly defined network protection against intrusion, disruption and denial of service attacks if you will CNA. Information assurance has a human dimension. For example, one of the biggest threats to the safety and security of any particular information system is the insider threat (that is, acts of treason).

The U.S. military's current doctrine and view is that the notions of computer network attack, exploitation, and defense should be embedded in one's thinking about the use of psychological or perception management operations. These should be integral parts of the thinking process in this area. They feel that the strategic warfare potential of IO could be much greater. There are some who believe that from a conceptual point of view it might be more useful to not conflate these issues under the term of Information Operation.

Strategic Warfare

We are in the midst of a very interesting debate about the nature of strategic warfare. The focus in the past has been on global strategic warfare. The old definition was related to nuclear weapons and trans-oceanic delivery of same, that is world war with the former Soviet Union.

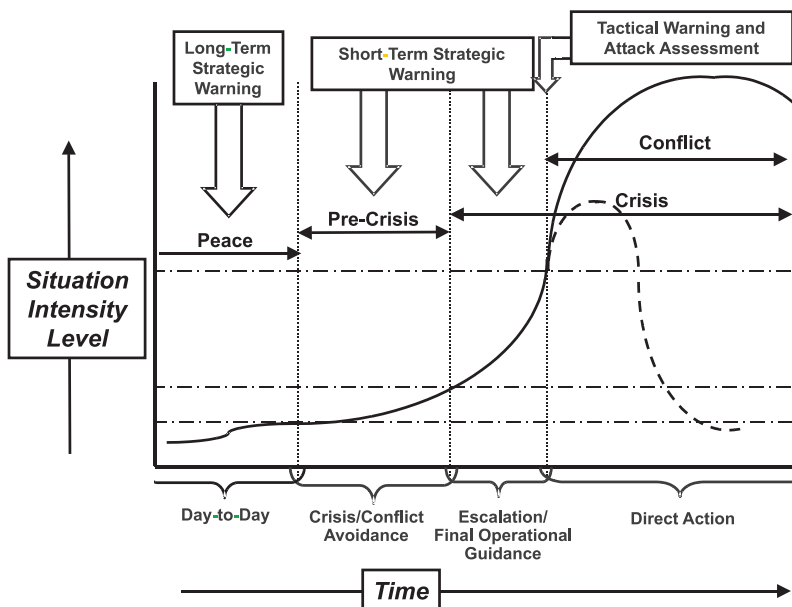
We saw a bipolar world. Even regional strategic warfare was based on large conventional forces and coalitions.

Now we are in a world of strategic (small “s”) concerns. This implies a much more complex, dynamic, and traditional view of strategic warfare. Strategies can now be highly asymmetric. We have no bipolar global rivalry. On a regional level, we see nuclear proliferation.

Figure 1 shows strategic and tactical warning in terms of a traditional situation intensity level and time. In the future we may face conflicts on the high end of the scale, which are more regional and strategic. For example, a serious conflict with China over Taiwan would likely be categorized by historians as the second Pacific War, that is, a regional strategic war. In the past, such as the 1996 crises over the Taiwanese elections, one would see a traditional mobilization and deployment of military forces such as carrier battle groups or the redeployment of mobile missile launchers.

Figure 1 shows a picture of how we will experience crises and wars of the future. They will be fairly well-structured. Each will have a pre-crisis period, a crisis period, and then a dramatic escalation phase.

Figure 1
Strategic and Tactical Warning



Unfortunately, in future wars and conflicts, information weapons will be used extensively by both nation states and non-nation states and/or individuals. Attacks through cyberspace may emerge with little strategic, operational, or tactical warning. Put simply, a period of cyberspace peace may be very noisy with many incidents. One of the challenges will be getting timely short-term strategic warnings, as well as tactical warning or attack assessment, when a serious act of malevolence emerges through cyberspace.

One of the CIP related challenges right now is how to define incident. We need to get the language right within the federal government. Even more challenging, the U.S. will have to work with key allies within the North Atlantic Treaty Organization to reach agreement among them about CIP related terminology. There are three important questions: What is an incident, how are we going to measure it, and how are we going to create an alert, warning, and response system?

During the fall of 1995, the intelligence community had a noteworthy intelligence failure that was a misappreciation of how rapidly global private industry could fix the Y2K problem in a variety of areas. Many of us at RAND, including myself, participated in a number of pre-Y2K exercises and were quite startled to see how rapidly, especially as the deadline loomed, some of these problems were dealt with. This reflects the highly dynamic global IT environment. Nation states such as the United States difficult a hard time comprehending this.

Key AWR Issues

The current Administration will have to address a number of key alert, warning, response (AWR) issues. The most fundamental issue is whether you can create alert, warning, response architecture. The day-to-day noise level is very high. We do have the beginnings of an intelligence community capacity to start giving people a sense of strategic warning. Long-term strategic warning is rough-hewn right now and has very uncertain timelines. Short-term strategic warning is based on activity in cyberspace, but suffers from a lack of indicators and experience. Tactical warning looks extremely difficult. Timely attack assessment, which includes perpetrator identification, magnitude of ongoing attack, and the possibility of future attacks, also looks difficult.

This is a very serious and challenging problem because information technology is evolving very rapidly. The target sets (i.e., the IT intensive infrastructures) are going through very rapid evolution because of

globalization, privatization, and the exploitation of this technology. Also, a particular infrastructure may have certain types of vulnerabilities today that in the future it may be able to solve, but in the process of modernizing and transforming itself it may produce new emergent vulnerabilities. In turn, these threats are highly dynamic. So one of the big challenges for the U.S. government is to try to develop a capacity to make credible forecasts about what the emergent CIP related threats will be.

We have had experience with incidents over the last couple of years (for example, the early 2000 Yahoo! denial-of-service attacks and this summer's Code Red worm). We have had mixed success as to whether we can, in fact, develop a tactical warning system that can provide information in a timely fashion so the recipients of that warning can have any capacity to make a meaningful response. There is considerable uncertainty about our ability to do this. A key element will be an increasing degree of global information sharing between the U.S. and its friends and allies. It may turn out that in the world of tactical warning the whole focus should be on how you can rapidly respond, rather than on whether you can count on that warning to provide you with sufficient time to make a meaningful response.

This is going to be very challenging. We discovered this during our RAND exercises, especially with senior decision-makers. One of the features of a future, possibly severe, political-military crisis is the involvement not only of nation states as opponents, but also many third parties including nation states, criminal organizations, public action or nongovernmental organizations, or individuals who for whatever reason conduct cyberoperations during the crisis. This is a powerful way to increase the fog of war. We may have an interesting paradox here. The military has touted the development of a revolution in military affairs (RMA) by deploying advanced command, control, communications, computers and intelligence (C4I) capabilities. This is the current revolution in military affairs. That "revolution" may give our military in the theater of operations "information dominance" or knowledge to conduct military operations that is superior to that of our regional military opponents. Ironically, the national command authority in Washington at the very time we might have superiority in this regard in the theater might be consumed by a fog of confusion of cyberevents that lead to major civilian infrastructure disruptions. For example, the ground traffic control systems in Manhattan could be disrupted along with a number of other major CIP related incidents while the President

is trying to decide whether to deploy forces to either the Pacific or the Persian Gulf.

We have found that when you introduce third parties, the issue of the non-timeliness of perpetrator identification tends to induce high-level decision making caution and delay. Therefore, it may turn out that one of the most strategically interesting ways to use information operations is to induce a fog of war at the national command authority level, rather than focus on trying to interfere with U.S. military forces. On the other hand, the future “just in time” logistics system in our military may well become priority targets for those who wish to use these cyberwarfare tools and techniques.

Key CIP Issues

The first key Critical Infrastructure Protection (CIP) issue is the blurring of security and law enforcement boundaries. One of the interesting issues that we have been exploring in some of our exercises is the possible emergence of a symbiotic relationship between transnational criminal organizations (which should be treated as very high-performance multinational corporations), terrorist organizations, and nation states. A good model of this dilemma is the ongoing debate about what we should do about the war in Colombia, where a symbiotic relationship exists between those who are selling drugs and those who are carrying out revolutionary political action such as the FARC (Revolutionary Armed Forces of Columbia). We see this elsewhere in the world as well. Cyber-warfare or cyber-techniques may well be new elements in this mix that will challenge the institutions of national security, law enforcement, and intelligence.

Another issue is uncertain and problematic threat assessment. The dynamic nature of targets and threats challenges us. As noted above, the CIP-related targets in the U.S. and elsewhere are undergoing very dynamic change. Simultaneously, new CNA tools and techniques are rapidly evolving.

Another challenge is that much of private industry is not convinced that a serious threat exists today. Private industry sees security as a cost center. They are under tremendous economic pressure to have a lean, taut enterprise, yet they might be excruciatingly vulnerable to disruption by a variety of forms from a variety of CNA tools and techniques

A major and ongoing challenge concerns the information exchange between private industry and the U.S. government. This is still unresolved even though the last Administration worked very hard on this issue.

Another issue is whether there will be a successful emergence of a confederation of information sharing and analysis centers (ISACs). These centers exist in the financial community, telecommunications, and other communities. But we are in the very early phase of this, both in their internal development and in their ability to communicate with each other and the federal government. There are several major problems to overcome if information sharing is more likely between private interests and public institutions.

Beyond that is the question about developing a viable U.S. government-private sector alert, warning, response system. We do not know yet if we can do this. The first attempt to do this was to create the National Infrastructure Protection Center (NIPC) inside the Federal Bureau of Investigation. So far, NIPC has gone through considerable growing pains.

It is also important that we develop an alert, warning, response system with our allies. That is an emerging challenge as to how we will operate with key allies during future political military crises. Key allies will be very important to us in our ability to project military power in an effective and timely manner in future crises or regional wars. If, for a variety of reasons, cyberweapon techniques knock an ally out of the war, this could have enormously disruptive effects even if our own information systems have not been disrupted or subject to attack. Providing protection, reassurance, and interaction with key allies during future contingencies is going to be a very important challenge.

As noted, there is a host of legal challenges associated with the evolution of the Freedom of Information Act (FOIA), antitrust laws, and other legislation. Private industry does not have a positive reaction when members of the federal government arrive and say they are "here to help." This is not surprising because in many cases private industry has grave concerns that critical data about their vulnerabilities will come into the public domain or call into question the reliability and credibility of their institutions. It is not surprising that banks do not talk to the government about information incidents very often. Private interests will be very concerned that FOIA will be used to compromise sensitive corporate data. The issues of anti-trust regulation will have to be addressed in infrastructure sectors are encouraged to share information.

Some Emergent R&D Issues

The United States government is going to have to spend more time helping to develop risk management frameworks and techniques both in the private sector and government sector. We are still in a very early stage in this regard. On the other hand, there is considerable work in this area. The federal government will have to develop a complete appreciation as to how much work has been done in private industry on this issue.

A second key issue is the modeling of interdependence for better risk assessment. As noted, the U.S. intelligence community thought there was going to be much more bad news involving Y2K failures, which did not happen. A much better understanding of the very dynamic nature of infrastructure vulnerability and threat will have to be developed.

Assessing the economic impact of computer network attacks is another challenge. How much damage and disruption can computer network attacks cause? Will it be nationally significant? It may be very significant to a particular corporation but, given the fact that we have a \$10 trillion economy, we have a fair amount of resilience.

Figure 2 **Some Emergent R&D Issues**

- Development of risk management frameworks and techniques
- Modeling of interdependence for better risk assessment
- Assessments of economic impact of CNA
- Interdependence modeling and metrics development vital pre-cursor for CIP action
- Development of tactical warning indicators and systems
- Development of timely attack assessment
- Secure communications and data bases to facilitate de-centralized information exchange

The question of interdependence modeling and metrics development is a vital precursor for credible CIP action. You will have to credibly argue to skeptical CEOs that they should pay for insurance for protection and response.

Development of tactical warning indicators and systems is another challenge. Within the RAND community a wide spectrum of opinion exists as to how feasible and likely this may happen. But this is an area where a major research and development (R&D) investment should be made. Associated with this is timely attack assessment, or perpetrator identification. A major investment in artificial intelligence (AI) tool and technique may help a great deal, but the payoff of this investment will likely remain uncertain until there is a major R&D investment.

We need secure communications and database management systems to facilitate a decentralized information exchange system. It is highly likely, in fact probable, that this will be a confederal process between the private industry sectors and the U.S. government. If you are trying to create a viable alert, warning, response system it is going to be a much more complicated and dynamic process.

Finally, the U.S. government will have to conduct extensive outreach to the private sector. The private sector dominates much of this technology and has dominant expertise both in creating new capabilities and a variety of responses.

Endnote

- * Contrary to some of the ideology that might be described as neo-Victorian conceit that information technology (IT) is an unalloyed good, I and a number of colleagues at RAND, especially Roger Molander, David Mussington, and Richard Mesic, have spent a great deal of time trying to imagine through the “Day After” exercise techniques how IT intensive infrastructures could malfunction or how this technology might be creatively exploited by individuals, nonstate actors, and state actors who use these tools and techniques for nefarious purposes.