

CHAPTER 22

INFORMATION TECHNOLOGY AND MILITARY AFFAIRS:

FRANCE, THE UNITED KINGDOM, AND NATO

By
Danielle Phillips

Throughout its history, NATO has based its defense planning and policies on the shared outlooks of and close cooperation between the political leadership and defense establishments of its member states. Cooperation has never been perfect, and outlooks have never been identical, but in the history of alliances, few have been as cooperative, as long-lasting, and as successful as NATO.

Formed primarily to deter and if necessary defeat feared Soviet aggression, NATO since the collapse of the U.S.S.R. has reinvented itself. Thus, at the April 1999 NATO Summit in Washington, held on the 50th anniversary of the founding of the organization, NATO adopted a new Strategic Concept that moved beyond the old conception of collective defense and encompassed comprehensive crisis management. Henceforth, NATO will not only defend its member states, but also move against threats to the values

that it espouses in areas of interest and importance to its member states. *Operation Allied Force*, the air war in the skies over Kosovo and the former Yugoslavia in 1999 in opposition to Serbian ethnic cleansing against Albanian Kosovars, was the first operational manifestation of the new doctrine.

Having withstood and surmounted the dangers of the Cold War and redefined its primary purpose for existence in the post-Cold War world, NATO in the early 21st century is the world's pre-eminent alliance. Nevertheless, it faces an insidious internal challenge born of the technologies of the Information Age.

That challenge results from the significantly different approaches some NATO member states are taking to what is called in the United States the "revolution in military affairs" (RMA), and to the diverging military capabilities that are developing within NATO as the result of different speeds and levels of application of the technologies of the RMA to different militaries. Much of the challenge results from differing viewpoints and policies on information warfare and information operations, and differing views on the impacts of advanced information and communication technologies on military affairs.

Indeed, as successful in an operational sense as NATO was in *Operation Allied Force*, the existence both of different approaches to Information Age warfare and of different levels of military capabilities was discernible there. Put simply, the United States shouldered the brunt of the burden of the air war at least in part because the military capabilities of other NATO states could rarely be integrated with the operational requirements of U.S. forces. It would be

ironic—and unfortunate—if the technologies of the Information Age proved to be the instruments of the decline of NATO.

Bounding the Issue

NATO's political leadership and planners are aware of the challenge and are attempting to address it. Indeed, at the December 1998 NATO Defense Ministerial Meetings, NATO defense ministers agreed to develop a defense capabilities initiative for the 1999 Washington Summit. The proposed initiative aimed at "developing a common assessment of requirements for the full range of military operations with a particular emphasis on technology and interoperability, especially in areas such as logistics and command, control, and communications." It also proposed to address "capabilities which are critical to the successful execution of joint military operations."¹

The language of the guidance did not make specific reference to information warfare, information operations, or the impacts of advanced information and communication technologies on military affairs. However, considering *U.S. Joint Vision 2010* and U.S. Secretary of Defense William Cohen's pre-ministerial push for NATO to examine its information technology capabilities, one can infer that information warfare and information operations were central issues at the root of this guidance.²

After the 1998 Ministerial, NATO at its 1999 Washington Summit detailed a new Strategic Concept and Defense Capabilities Initiative.³ These are steps in the right direction. However, it is far from certain that the potential of either will be fully realized. Within NATO, there are

significantly different views on many issues regarding the RMA and its implications, not the least of which different views concerning information warfare, information operations, and the impacts that Information Age technologies will have on military affairs.⁴

Indeed, the belief that an information technology based revolution in military affairs is well underway and advancing rapidly is primarily held in the United States, and to a similar but lesser degree the United Kingdom. The concept of an RMA is often met with hesitation, skepticism, and even outright resistance by many of NATO's European members.

At the same time, NATO is expanding its sphere of influence and increasing its operational reach just as its member states are experiencing across the board reductions in defense spending and military capabilities. A number of NATO nations have revised their national defense strategies to take into account the radically different international security environment and the need for force modernization in light of Information Age technologies. Even so, the degree to which individual national defense thinking and capabilities are being modernized varies from state to state.

A few states, led by the United States and to a lesser degree Great Britain, have accepted the RMA as the inevitable wave of the future of warfare. They are incorporating advanced Information Age technologies into their armed forces at moderately high to extremely high rates of speed. They also are adapting their tactics, operations, and military doctrines to those technologies and the capabilities they provide, even if

more slowly than the more forceful advocates of the RMA would prefer.

Other states, notably France and many smaller NATO nations, are proceeding more slowly still, both in the rate of incorporation of new technologies and in the adaptation of tactics, operations, and doctrine. Some do not accept conceptually or philosophically that an RMA driven by advanced information and communication technologies is in the offing. Others see in the post-Cold War world advantages in developing a separate European security and defense identity with European-oriented security and defense strategies and doctrines. Almost all are constrained in the amount of new technology they can incorporate in their militaries because of reductions in military budget.

For NATO, this is potentially dangerous. To the extent that different NATO states obtain different military capabilities and adopt different strategies and doctrines based on those different capabilities and different views of the future of warfare, the shared outlooks and close cooperation that bound NATO together during the Cold War have potential to diminish during the early years of the Information Age.

To reiterate, as successful in an operational sense as NATO was in *Operation Allied Force*, the beginning of such a phenomenon was discernible there. It would be ironic—and unfortunate—if the technologies of the Information Age proved to be the instruments of the decline of NATO. This study will explore this challenge in several ways.

First, it will examine the perspectives and policies of two European NATO states, the United Kingdom and France,

on information warfare, information operations, and the role and impacts of Information Age technologies in and on warfare. Given that these technologies are central to the economic transformations taking place in the United Kingdom, France, and other European states, the study will also explore some of the changing interrelationships between defense industries, military establishments, and advanced information and communication technologies.

Second, the study will also assess the implications of those perspectives and relationships for NATO's future. Unless handled carefully and correctly, the presence of significantly different outlooks and undertakings on information warfare and information operations within and between NATO's 19 nations has potential to weaken if not disrupt the alliances ability to function.

Finally, the article will conclude with a set of recommendations designed to help NATO maintain its cohesion as the alliance moves deeper into the Information Age.

The United Kingdom: Views and Policies

Of all of NATO's European members' viewpoints and policies on information warfare, information operations, and the impacts of advanced information and communication technologies on military affairs, the United Kingdom's perspective is in most respects the closest to that of the United States. From the British perspective, the biggest change in the conduct of future military operations is likely to come from a combination of improved weapons and weapons capabilities and from the application of information technology to military command and control.⁵ This in turn, official British

spokesmen maintain, has potential to transform the way that 21st century wars will be fought.

Doctrine, Policy, and Programs

This perspective developed over time, but was finally codified in 1998 when the United Kingdom concluded its *Strategic Defense Review*. The review marked a significant departure from the United Kingdom's previous defense posture. Under the auspices of the 1998 review, the United Kingdom is pursuing a program of force modernization that will develop new generations of weapons that incorporate Information Age technologies. The incorporation of Information Age technologies into the military structure is part of the British Ministry of Defense's plan to develop an efficient, top-of-the-line, cost-effective force posture.

The *Strategic Defense Review* identifies a number of military capabilities as important to force development. Among the most prominent in the British strategy are those associated with information warfare and information operations, especially command, control, communications, and computers. The British also see intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) as critically important. Some of the capabilities contained within the new force posture include the Airborne Standoff Radar Surveillance System (ASTOR) and an indirect fire precision attack program including "smart, long-range, guided weapons delivered by rockets or extended range artillery."⁶ The British program also incorporates increased use of stand-off weapons and unmanned platforms such as unmanned vehicles for aerial reconnaissance and the removal of mines on land and at sea.

The British are also taking steps to address potential weaknesses resulting from increased reliance on technology. For example, recognizing that “increased automation of tasks” can increase vulnerabilities by reducing the situational awareness of human operators, the British have implemented programs designed to train and educate personnel involved with advanced technologies.⁷ In addition, the United Kingdom has initiated programs such as the Joint Battlespace Digitization initiative, which is designed to “improve operational effectiveness by integrating weapons platforms, sensors, and command, control, intelligence, and information systems.” It is based on the belief that in the future, military operations will be merged into joint operations rather than take place in separate battlespaces under the domain of individual armed services.⁸

In light of these advancing military capabilities and the perceived changing face of battle, the British military also recognizes the need for doctrinal evolution to maintain overall force effectiveness. To accomplish this, Ministry of Defense officials are working in close conjunction with the U.S. Department of Defense to explore and to further develop policy and doctrine for the United Kingdom’s evolving national security and defence policy strategy.

The British Ministry of Defense is confident that it can incorporate Information Age capabilities into its national security posture despite a downward trend in British defense expenditures. One way to accomplish this is by incorporating off-the-shelf civilian and commercial capabilities into military equipment, especially in the areas of information and communication technologies. The British defense

establishment recognizes that with “civil investment in research and development 10 × greater than [that of] defense investment” in the fields of electronics, software and information technology, “new advances in the civil market are increasingly having profound implications for [their] future military capability.”⁹ This is a significant change from the traditional British (and American) pattern in which capabilities developed by the military were later transferred to the private sector.

The Defense Industrial Sector

Indeed, the United Kingdom has formally adopted this changed perspective as formal policy. Thus, guided by the *Strategic Defense Review*, the United Kingdom also established a Defense Diversification Agency designed to promote civil-military joint ventures, research partnering, and development of dual use technologies. One of the chief target areas for the agency is information and communication technologies.

The objective of the Agency is not only to incorporate advanced Information Age technologies into British weapons and defensive systems. It also clearly seeks to help British industry. Since the mid-1980s, British defense spending has been cut 33 percent. These reductions have impacted not only overall defense policy, but the British defense industrial base as well. The Defense Diversification Agency aims to preserve and promote British defense industries through a civil-military program of technology transfer designed to “get the most out of defense technology.”¹⁰ The British clearly feel that the defense industry should diversify and adapt to the changing security and economic environment.

The Defense Diversification Agency will promote dual-use research and a formal system of technology

transfer between the private commercial sector and the military. It will not only promote the incorporation of civilian technologies into military capabilities, but also the diffusion of military technologies into the private sector. The agency plans to develop a database containing “a wealth of knowledge within MOD about future equipment needs, about technological trends, about sources of advice and assistance, and about relative market assessments.” This knowledge will be made available to companies so that they can “exploit potential new opportunities for their products, technologies, and skills in the UK and overseas military and civil markets.”¹¹

The Defense Diversification Agency also makes provisions for a Defense Diversification Council chaired by a prominent industrial leader, “with a membership drawn predominantly from industry but including also the Chief Executive of DERA and other appropriate representation from central and local government and from trade unions.”¹² In addition, the Agency will create Technology Diversification Managers who will work directly with local industries to “build a collaborative relationship in order to ‘broker’ technology activity between DERA and local small and medium enterprises.”¹³

Overview

Clearly, the United Kingdom’s approach accepts the reality of immense change, even an RMA, in military affairs and economic affairs driven by Information Age technologies. Although the United Kingdom is only at the beginning stages of formalizing information warfare and information operations doctrine, it is pursuing programs that will incorporate weapons and

capabilities that will require such doctrine into its defense inventory. It has also identified a strategy and created an organization that aims to harness and incorporate the best civilian technologies into military capabilities, thereby ameliorating the impact of the drawdown in its defense budget. It has created and is implemented training programs designed to enhance the ability of British soldiers, sailors, and airmen to master new required skills. The United Kingdom, in other words, appears to have accepted the inevitability of an RMA driven by Information Age technologies, and is adapting its defense posture accordingly.

France: Views and Policies

France's views and policies on information warfare, information operations, and the impacts of advanced information and communication technologies on military affairs are also evolving. However, they are evolving more slowly than the United Kingdom's views and policies, and in certain important respects are markedly different from those of the United Kingdom. Even though France is not a participant in NATO's integrated military structure, its views and policies on these issues are vitally important for several reasons.

First, France is a major player in European affairs and global military affairs, and its outlooks and positions carry significant influence on the continent. Second, France's involvement in NATO military affairs significantly increased during the 1990s. In the post-Cold War world, France has again become a critical player within NATO. Third, France is one of the leading promoters of the European Security and Defense Identity (ESDI) within the European Union. ESDI

carries significant importance for both the EU and NATO. And finally, France's defense industries are pillars of Europe's defense industrial capacity, and French science and technology and its application to weapons and defense systems has long been at the forefront of European and global military affairs. Thus, the French perspective on information warfare, information operations, and the role of advanced information and communication technologies in the military can not be overlooked.

Doctrine, Policies, and Programs

Like the United Kingdom, France is pursuing a program of force modernization. However, at least rhetorically, France's modernization efforts concentrate more on improving existing capabilities than on developing new generations of weapons that have potential to transform the way that wars are fought. Many in France feel that "information warfare [and information operations—author] is one of the essential instruments in France's sovereignty and independence, one of concern not only to the defense industry, but also the economy, media, science, and culture."¹⁴

Many in the French defense establishment recognize the importance of developing an information technology strategy, but this recognition does not necessarily carry over into a publicly stated intention to develop an information warfare or information operations strategy. The thrust of French efforts appears focused mainly on the role of information and communication technologies in commerce, the economy, and society, not defense. Although France's overall concept of information warfare falls in line with American schools of thought, France, unlike the United

States and the United Kingdom, has yet to publicly incorporate an information warfare strategy into its overall defense programming.

Nevertheless, French military planners and thinkers are well aware of the need to accelerate their planning and preparations for new types of warfare. As long ago as 1996, senior French defense and armaments industry officials began to become concerned that France was lagging behind on the information warfare front. General Jean Philippe Douin, former Chief of Staff for the French Armed Forces, announced in an internal memo that “a new type of warfare was coming to the fore.”¹⁵ To remain competitive at the industrial level as well as in security circles, he posited, France needed to seriously examine its information technology capabilities and develop a coordinated information warfare strategy. Shortly thereafter, the Centre d’Electronique de l’Armement (CELAR) officially assumed the lead for French information warfare strategy.

By the late 1990s, CELAR had become France’s “technical center of the war of information for defense.”¹⁶ However, CELAR’s primary research and development activities lie in the traditional areas of electronic and optronic warfare. Thirty eight percent of its work is dedicated to these fields, with 8 percent designated to optronic and electronic component development. Other areas in which CELAR specializes are information systems, telecommunications, and information system security. Only 33 percent of this work focuses on information and communication systems combined, while the remaining 21 percent is dedicated to security.¹⁷

However, even though CELAR has an input in all programs involving information technology, it does not

actually set information technology strategy, nor does it have authority over other agencies that work on information technology or information warfare issues. These other agencies include the Direction des Affaires Strategiques (DAS) and the Ecole Polytechnique's Centre de Recherche et d'Etudes Scientifiques et Techniques (CREST). Each agency acts individually, with little to no harmonization of efforts. Through at least 1996, there was "no official body to dovetail all the [infowar] undertakings, leaving each organization to work in relative isolation" on issues of information warfare and information operations.¹⁸

Despite these impediments, information warfare and information operations have arguably gained greater importance in French defense thinking and policy. By the end of 1997, the technology used by the French military had become increasingly similar to civilian capabilities, indicative of a recent migration toward the incorporation of civilian technologies into the military structure.¹⁹ In 1998, the French army began to increase its focus on incorporating improved information and command systems into its structure.²⁰ Although French spokesmen have inferred that one of France's ultimate goals with regard to information capabilities is to be able to glean real-time information and deploy resources and forces to meet threats as soon as possible, this is not necessarily an information warfare or information operations strategy.

As intimated above, France's recent steps forward in thinking about and planning for information warfare and information operations have been translated into defense programs in only a limited way. France's defense program remains based on a strategic vision for national defense enunciated in 1995, before the

more recent emphasis on the role of Information Age technologies in warfare. Designed to look 20 years into the future, France's 1995 defense programming bill redefined the role and structure of the armed forces as well as the concept of French national security as a whole. Developed to address France's changing security and defense needs in the context of the evolving international security environment, France's programming bill outlined four strategic components of national defense: protection, deterrence, prevention, and projection. None of these clearly embraced information warfare or information operations concepts or capabilities.²¹

"Protection" concentrated on the defense of French territory. Major components consisted of controlling the trilateral approach to territorial defense, development of surveillance, and protection against threats.

"Deterrence" is "at the heart of France's defense strategy." It relied and relies on two "reduced and modernized components:" a submarine capability and an air capability.

"Prevention" of conflict revolves primarily around political actions. However, it involves military aspects as well, including intelligence, technical cooperation, and pre-positioning of forces.

"Projection" of power involves rapid deployment of forces outside France's national territory. It includes a stated need to attain the capability to deploy quickly a land component outside France of over 50,000 troops for NATO operations or 30,000 in a main theatre. It also includes a naval force projection capability of a "service group with its backup and a submarine force over a distance of several thousand kilometers," and

air projection of an “air transport capability maintained at the current level, [which is approximately] 100 combat aircraft and the corresponding refueling aircraft, air traffic control and detection means, and two air bases.”

In comparison to France’s past force structure, these four objectives are to be achieved by a radically altered military structure. Most noticeably, the size of French armed forces will be drastically reduced.

By 2015, the French army will be reduced from a 1995 level of 271,500 to 170,000, a 37 percent reduction.²² The French army will reduce its organizational structure from nine to four divisions, with as many as 38 operational regiments set to be disbanded by 1999.²³ However, it plans to incorporate field surveillance and data processing equipment to reinforce its “balanced division of heavy tanks and light tanks supported by Tigre helicopters, along with an increased range in precision of long-range weapons.”²⁴

Likewise, the French Navy will be reduced by approximately 20 percent, and the air force by slightly more than 25 percent. In addition to reductions in manpower, the navy will undergo a reduction in tonnage and number, as 13 ships will be decommissioned early. The Air Force will concentrate on projection capabilities and adopting new operational modes. Various groups within the air force will be disbanded by the end of 1999, including the Albion First Strategic Missile Group, the surface to surface ballistic nuclear component, and the Toul-Thouvenot air engineers regiment and support base. The Toul-Rosieres and Contrexeville air bases will be transformed into air detachments.²⁵

As this transpires, France plans to embark on improved training, incorporating a plan of military professionalization, gradually phasing out compulsory service and consolidating military equipment and organizational structures in each sector of the armed forces. The goal is to create a small, efficient, effective military.

However, unlike Britain's program, the French program appears to concentrate more on upgrading old systems and introducing advanced versions of already deployed systems. For example, included among the 1999 defense budget projects are the modernization of 13 Eridan class minesweepers, the development of improved air to surface missiles with improved propulsion and guidance capabilities (the ASMP), and the renovation of the command and control systems for a number of aircraft.²⁶ Thus, the French defense plan is instructive as much for what it does not say as for what it does say. It includes few new weapons systems or defense capabilities that are heavily dependent on new Information Age technologies.

France's 1999 military research and development budget provides a good case in point. While the 1999 defense budget designates 5.485 billion French francs for research and 15.604 billion francs for development, there is no publicly specified designation for the new information warfare related capabilities. Nor is there any reference to development of new revolutionary types of warfare, either operationally or in doctrine and strategy. Instead, France's modernization appears to focus on more traditional improvements in areas such as electronic and aerospace warfare, as well as improving existing capabilities rather than developing new ones.

The Defense Industrial Sector

This is evidenced not only by budgetary trends, but also by the publicly stated goals of the newly restructured defense industry. This restructuring was necessitated by the need to adapt to the drastic cuts France has made in its overall defense budget. Indeed, the restructuring of France's national defense industry is actually one of the components of France's overall defense strategy. The government has identified three fundamental goals to be achieved through the restructuring:

1. preserving "the integrity of industrial, technological, and human capital whilst developing essential synergies; preserving the interest of national defense;"
2. opening "new development perspectives;" and
3. pursuing and reinforcing "the policy of alliances, reunions, or fusions which have already taken place on a European level."²⁷

This redesigned defense industry is intended to serve as a vital player in France's modernization effort economically, industrially, and politically. The privatization of Thomason SA, the 1998 merger of Dassault Aviation and Aerospatiale, and the 1999 merger of Aerospatiale and Matra to form Aerospatiale Matra evidence the French commitment to restructuring the defense industry in order to remain competitive regionally and globally. Though the new face of the French defense industry is to be "a government reinforced industrial structure, particularly in the field of high technology," the main focus thus far has primarily been in the fields of aerospace,

aeronautics, and electronics, not advanced information and communication technologies.²⁸

The promotion of French and European defense industries is a byproduct of the European Union's European Security and Defense Policy. France in particular would like EU members to develop the security structures and military capability to conduct crisis management operations on its own if the United States and NATO opt not to become involved. For this to become a reality, a strong, unified defense industrial base is needed.

Inherent in this concept is a degree of increased independence from the United States both at the security planning and the defense industrial levels. In 1997, France joined the United Kingdom and Germany in identifying and implementing a trilateral initiative to promote the competitiveness of European defense industries to serve as a David to the United States defense industries' Goliath. One of the primary objectives in merging DASA and Aerospatiale Matra, as well as the other defense industrial consolidations that swept across Europe in 1999 was to create a defense base that could successfully compete with U.S. defense industrial rivals.

This initiative may be beginning to bear fruit. In the late 1990s, France began to increase its development of information warfare capabilities at the industrial level. Dassault in particular has made major contributions in terms of battlefield knowledge and rapid information processing. Yet the French defense industry has only minor influence on the overall state of defense policy, at least with regard to information warfare. Major defense contractors such as Thomson,

Matra, Alcatel, Giat Industries, and Dassault “are represented by just a single consultative and largely informal committee.”²⁹

Overview

France, then, presents a study in contrasts in its positions on information warfare, information operations, and the impacts of advanced information and communication technologies on military affairs. French military leaders and thinkers are fully aware that major changes are taking place in the conduct of warfare, many driven by Information Age technologies. Nevertheless, at least in public, the French Ministry of Defense has yet to develop and incorporate information warfare and information operations doctrine, strategy, and tactics into its overall defense planning. While France has gradually come to recognize the importance of information warfare and information operations, the fruits of this recognition have yet to ripen despite a recent acceleration in this regard. To reiterate, then, when compared with the United Kingdom and the United States, it is apparent that the critical issue for France is not so much what has done with regard to information warfare and information operations, but what has not been done.

Implications for NATO

The differences between British and French perspectives and policies on information warfare and information operations are indicative of those that exist among and between other NATO members as well. In addition, many smaller NATO states have neither the economic wherewithal nor the technological

capability that might allow them to incorporate significant quantities of Information Age technologies into their military forces. This, in turn, acts as an inhibitor on doctrinal, strategic, operational, and tactical change. As we have seen, this is the case even in a country such as France that has a highly developed technological, industrial, and military base.

This could create serious difficulties for NATO as it attempts to structure and organize its forces and capabilities for 21st century contingencies. Thus, while France recognizes the military importance of advanced information and technologies, it has yet to fully integrate them into its military strategy, doctrine, or forces. Conversely, the United Kingdom and the United States are molding defense strategy around advances in Information Age technologies. To reiterate, it is not necessarily what the French have said and done, but rather what they have not said and done.

What does this mean for NATO?

If advances in information technology are in fact changing the face of military affairs, national military planners must be prepared to abandon traditional thoughts on war and adapt a new defense paradigm. Such a new defense paradigm will contain not only new concepts of military capabilities, but also of organizations and even the very concept of war itself. Therefore, if as prevailing thought in the defense intellectual communities in the United Kingdom and the United States suggests, we are in the midst of a revolution in military affairs driven by information and communication technologies, NATO must revolutionize its thinking and its capabilities to maintain military effectiveness.

The problem with this is that the very nature of NATO force planning is such that NATO cannot dictate defense policies to its member nations. Therefore, if the military capabilities of NATO are to be revolutionized, a revision of the defense strategies and force postures of NATO members at the national levels must occur first.

The problem facing NATO is how national defense ministers and the defense establishments of all of its member nations can be convinced to accept information warfare and information operations both philosophically and conceptually.

But the problem does not end there. Once the defense establishments of NATO's member nations accept information warfare and information operations philosophically and conceptually, they must either increase defense spending or redirect and refocus it toward Information Age technologies that are at the core of the RMA. Given that the downward trend in defense spending since the end of the Cold War is unlikely to be reversed absent an immediate identifiable threat, refocusing and redirecting will undoubtedly be required. And even though information warfare and information operations may be more cost effective than previous types of warfare since civilian and commercial technologies can be incorporated into military postures relatively inexpensively, the initiative to integrate these technologies must first be taken by higher levels of government.

In other words, it must be a top down process. While industries may provide the technological capabilities, they cannot dictate national defense policies. It is thus imperative for industries to have a high level of

involvement in the defense planning process if NATO nations wish to successfully incorporate civilian capabilities into military systems. But as we have seen, there are different approaches to this within NATO. While the United Kingdom encourages and facilitates a high level of industry involvement through forums such as the Defense Diversification Council, France incorporates industry only minimally and through largely informal channels.

The degree to which individual NATO nations will be able to involve industry in their defense programs will, in large part, determine the degree to which each nation will be able to develop an authoritative, decisive information warfare and information operations strategy. It will also help determine the degree to which each nation will be able to successfully develop information warfare and information operations capabilities in and of themselves. If there are significant disparities in information warfare capabilities among NATO member nations, the Alliance will arguably face serious problems in terms of overall effectiveness and in terms of interoperability. Therefore, NATO nations need to ensure that their information warfare developments are at least somewhat coordinated. This will not only reduce duplication of efforts, but also ensure the interoperability of forces.

Conclusions

At present, the United States leads NATO with regard to information warfare and information operations capabilities, with the distance between the United States and its European counterparts immense. This is a dangerous situation for NATO. Unless

homogenized and coordinated, the different military tracks pursued by members of NATO will inevitably result in significant interoperability problems due to disparities in military capabilities. It will become increasingly difficult to maintain “separable but not separate” forces.

The United States and the United Kingdom are preparing to fight a new type of warfare, with a new class of weapons, with new doctrines. Meanwhile, other NATO states are not pursuing this course of action. The prospect of a NATO operation in which some members are prepared to fight Information Age warfare with state of the art equipment and doctrine, while other members and partners possess only 20th century capabilities is a daunting one which the Alliance must address.

If the United States is leading this revolution, how then can the outlooks, policies, and technologies of the U.S.'s NATO allies and partners be synchronized, if not harmonized, with those of the United States, and for that matter, the United Kingdom?

This is an extremely tricky issue. If not handled delicately and diplomatically, the RMA, information warfare, and information operations affairs could create a divide between “Fortress Europe” and “Fortress America.” A push to bring European Allies up to American standards runs the risks of creating an intellectual divide between the United States and United Kingdom on the one hand and the rest of NATO on the other hand. Similarly, considering the European push to develop ESDI and promote the independence of European defense industries, an effort to “Americanize” information warfare and information

operations standards and capabilities could fuel competition between industries. This would undermine rather than promote the national and industrial coordination needed if the alliance is to develop a unified, compatible, and capable information warfare and information operations capability.

Consider for example, the British, French, and German public commitment to creating an independent, competitive European defense industry which would be able to successfully compete against the American giants. While the United Kingdom recognizes U.S. dominance in the field of information technology, has publicly acknowledged that the United States will lead the way in this field, and is prepared to follow the U.S. lead, there is little evidence that other major NATO states are prepared to follow suit. Though the United Kingdom may presently be prepared to embark upon collaborative, coordinated efforts with the United States in information warfare and information operations, continued pressure from other European partners to promote European independence from and competition with American defense industries may place the United Kingdom in a position in which it is forced to choose between the United States and its European partners.

This competition and subsequent uncoordinated development of military capabilities poses a potential defense dilemma not only for the United Kingdom, but also for NATO. NATO states including France are committed to the concept of force and systems interoperability. However, for interoperability to become a reality as new capabilities are brought on line, it is imperative that defense strategists, planners, and industries work in conjunction with one another to develop

complimentary and compatible strategies, plans, and technologies, and to avoid a duplication of effort.

At its 1999 Washington Summit, NATO unveiled a Defense Capabilities Initiative designed to improve “interoperability and sustainability among Alliance forces...[and to] ensure that the military forces of the Allies remain on the same wavelength and able to move distances effectively and quickly.”³⁰ The effectiveness of this, or any NATO initiative, is determined by commitment at the national level to making that initiative a reality. In spite of dwindling defense budgets, the European Allies appear to have placed a new emphasis on improving their capabilities and increasing their share of the Alliance’s burden.

The political rhetoric to support increasing capabilities has reached new levels in European capitals. This is in large part due to *Operation Allied Force*, in which European deficiencies were glaringly illustrated. As a result, the Allied focus on capabilities has reached a fever pitch—but not in respect to information warfare capabilities. Rather, the capabilities the Europeans have designated with “must have” status are items such as strategic lift, precision guided munitions, and the like. It is important to note, however, that defense budgets have yet to reflect this new trend.

In light of constrained budgets and the EU’s commitment to deploying and sustaining a 60,000 man force capable of carrying out Petersberg Tasks by 2003, any marked improvement in capabilities will likely be in support of peace keeping and crisis management missions. It is unlikely to be in areas such as information warfare and other revolutionary battle scenarios. Unless NATO’s European members

determine that information, communications, and logistics are primary foci of their national defense strategies, and budgetarily commit themselves to developing these capabilities, the force posture of NATO's European members will not be able to meet the requirements of the American conception of 21st century warfare.

¹NATO Defense Ministerial Press Communiqué. M-NAC-D-2(98)152. December 17, 1998.

²At the Department of Defense Concept Development and Warfighting Conference, Cohen publicly advocated NATO modernization and restructuring to develop four core capabilities—mobility, effective engagement, survivability, and interoperability—by “improving command control, and communications, logistics, and interoperability.” Cohen also insisted that members should share technological innovations as “a military force is only effective as its flow of information.

³See *The Alliance's Strategic Concept*, NATO Press Release NAC-S(99)65, and *Defence Capabilities Initiative*, NATO Press Release NAC-S (99)69.

⁴Linda D. Kozaryn, “NATO Needs More Mobility, Better Ammo,” *Defense Press Service News*, November 19, 1998.

⁵*United Kingdom Strategic Defense Review* (London: Ministry of Defense, 1998), p. 37.

⁶*Ibid.*

⁷*Ibid.*

⁸*Ibid.*

⁹*Ibid.*

¹⁰*Ibid.*

¹¹*Ibid.*

¹²*Ibid.*

¹³*Ibid.*

¹⁴“France Advances on Infowar Front,” *Intelligence Newsletter* Volume 289. (June 6, 1996).

¹⁵*Ibid.*

¹⁶La Delegation Generale pour l'Armement, at <http://www.defense.gouv.fr>

¹⁷“France Advances on Infowar Front,” *Intelligence Newsletter*, Volume 289 (June 6, 1996).

¹⁸*Ibid.*

¹⁹“Ever Faster Move to Dual Use Tech,” *Intelligence Newsletter*, Volume 324 (December 4, 1997).

²⁰“Infowar the Star at Eurosatory Show,” *Intelligence Newsletter*, Volume 337 (June 18, 1998).

²¹“The Various Aspects of our Defense Strategy,” at <http://info-france-usa.org/profil/glance/def97/various.htm>

²²“The New-Style Armed Forces,” at <http://info-france-usa.org/profil/glance/new.htm>

²³“Reorganization of the Forces from 1997 to 1999,” at <http://info-france-usa.org/profil/glance/def97/reorgani.htm>

²⁴“The New-Style Armed Forces,” at <http://info-france-usa.org/profil/glance/new.htm>

²⁵“Reorganization of the Forces from 1997 to 1999,” at <http://info-france-usa.org/profil/glance/def97/reorgani.htm>

²⁶*Annual Report: Le Projet de Budget de la Defense pour 1999* (Paris: September 9, 1998).

²⁷“A New Start for the Defense Industry,” at <http://info-france-usa.org/profil/glance/start2.htm>

²⁸*Ibid.*

²⁹“France Advances on Infowar Front,” *Intelligence Newsletter*, Volume 289 (June 6, 1996).

³⁰Speech by NATO Secretary General, Dr. Javier Solana, “NATO: Its 50th Anniversary—The Washington Summit—The Next Century,” January 25, 1999.