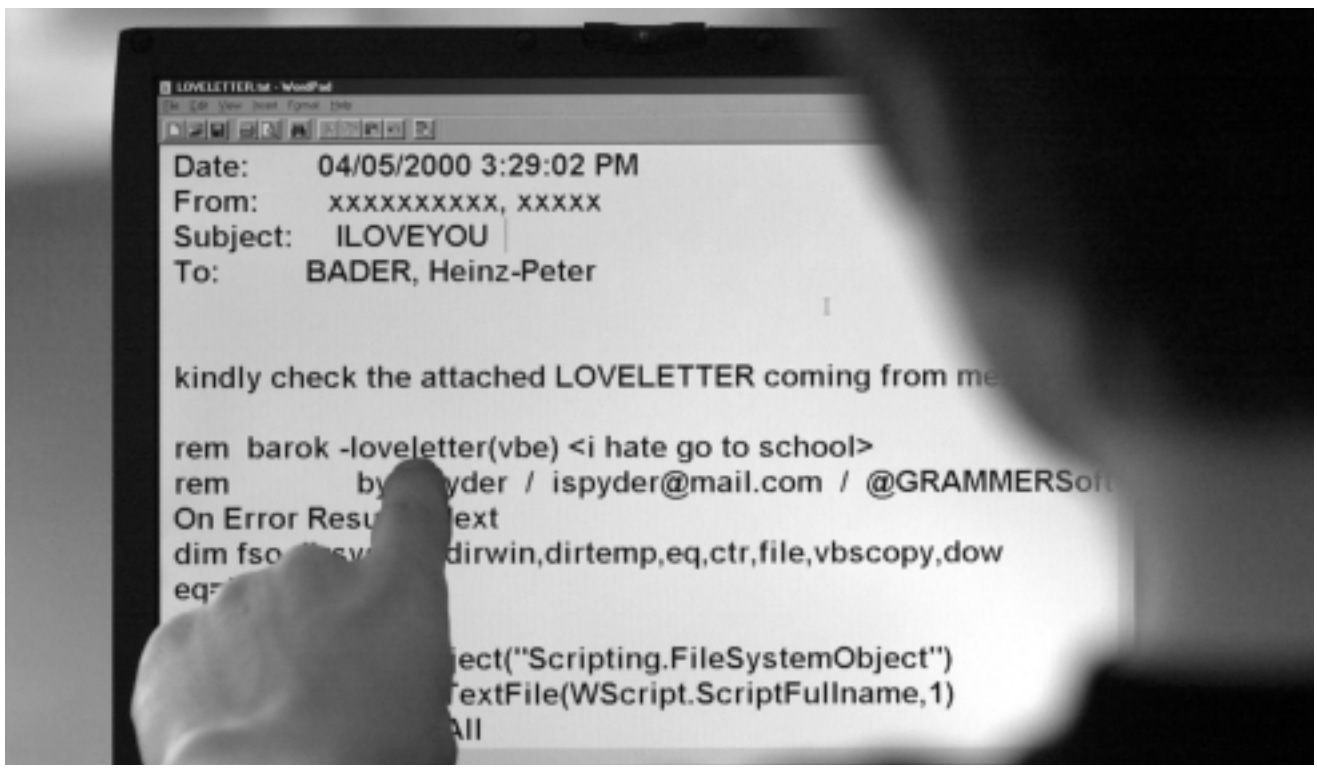
Countering cyber war

Timothy Shimeall, Phil Williams and Casey Dunlevy argue that defence planning has to incorporate the virtual world to limit physical damage in the real.



Viral attack: Disruption of information infrastructures is an attractive option for countries that lack the capacity to compete on the traditional battlefield

For many, the term cyber war conjures up images of deadly, malicious programmes causing computer systems to freeze, weapon systems to fail, thwarting vaunted technological prowess for a bloodless conquest. This picture, in which cyber war is isolated from broader conflict, operates in an altogether different realm from traditional warfare and offers a bloodless alternative to the dangers and costs of modern warfare, is attractive but unrealistic. Such a scenario is not beyond the realm of possibility, but it is unlikely. Cyber warfare will almost certainly have very real physical consequences.

As computer technology has become increasingly integrated into modern military organisations, military planners have come to see it as both a target and a weapon, exactly like other components and forces. Like other elements of the modern military, cyber forces are most likely to be integrated into an overall battle strategy as part of a combined arms campaign. Computer technology differs from other military assets, however, in that it is an integral component of all other assets in modern armies. From this perspective, it is the one critical component upon which many modern militaries depend, a dependence that is not lost on potential enemies.

Countries around the world are developing and implementing cyber strategies designed to impact an enemy's command and control structure, logistics, transportation, early warning and other critical, military functions. In addition, nations are increasingly aware that the use of cyber strategies can be a major force multiplier and equaliser. Smaller countries that could never compete in a conventional military sense with their larger neighbours can develop a capability that gives them a strategic advantage, if properly utilised. As a RAND Corporation study pointed out in the mid-1990s, the entry costs for conducting cyber war are extremely modest. Not surprisingly,

Timothy Shimeall is a senior analyst with the CERT Analysis Center of Carnegie Mellon University, Pittsburgh, Pennsylvania, with specific interests in cyber war and cyber terrorism. Phil Williams, a former NATO fellow, is a professor at the University of Pittsburgh and a visiting scientist at the CERT Analysis Center. Casey Dunlevy is a former intelligence analyst, and leads the CERT Analysis Center.

therefore, countries that are not as dependent on high technology within their military establishment consider such dependence a potential "Achilles heel" for their enemies.

Advanced, post-industrial societies and economies are critically dependent on linked computer information and communication systems. Sophistication has itself become a form of vulnerability for enemies to exploit. Disruption of civilian infrastructures is an attractive option for countries and non-state actors that want to engage in asymmetric warfare and lack the capacity to compete on the traditional battlefield. Indeed, so important are information infrastructures that more and more nations consider an attack against them the equivalent of a strategic strike.

Traditional lines between war and peace are becoming blurred. This development was presaged by the Cold War, but is even more obvious in the war against terrorism in the wake of the 11 September attacks on the World Trade Center and the Pentagon. It suggests that the computerised information systems of NATO member states are likely to be the continuing target of attacks by a non-traditional enemy, whose main goal is physical destruction and disruption and who is likely to exploit vulnerabilities wherever they are to be found.

In this connection, it is worth emphasising that cyber war is not the defacement of web sites owned by a rival nation, organisation or political movement. Even when they accompany other tensions or hostilities — as they did during NATO's Kosovo air campaign in 1999 — such attacks on web sites are best understood as a form of harassment or graffiti and not as cyber war *per se*. There are, nevertheless, several levels of cyber war, of which three stand out: cyber war as an adjunct to military operations; limited cyber war; and unrestricted cyber war.

When modern military establishments are involved in military hostilities, a key objective is to achieve information superiority or information dominance in the battle space. This requires suppressing enemy air defences, blocking and/or destroying radar, and the like. The aim, in Clausewitzian terms, is to increase the "fog of war" for the enemy and to reduce it for one's own forces. This can be achieved through direct military strikes designed to degrade the enemy's information-processing and communications systems or by attacking the systems internally to achieve, not denial of service, but a denial of capability. In effect, this form of cyber warfare focuses almost exclusively on military cyber targets.

In a limited cyber war, the information infrastructure is the medium, target and weapon of attack, with little or no real-world action accompanying the attack. As the medium of attack, the information infrastructure forms the vector by which the attack is delivered to the target — often through interconnections between the enemy and its allies, using links for sharing resources or data, or through wide-area network connections. Alternatively, an inside agent might place malicious software directly on the enemy's networks.

As the target of attack, the infrastructure forms a means by which the effectiveness of the enemy is reduced. Networks facilitate organisational missions. Degrading network capacity inhibits or prevents operations that depend on the network. Degrading the level of service on the network could force the enemy to resort to backup means for some operations, which might expose additional vulnerabilities. Degrading the quality of the data on a network might even force the enemy to question the quality of the information available to make decisions. As the weapon of attack, the infrastructure could be perverted to attack itself — either via the implantation of multiple pieces of malicious software, or via deliberate actions that exploit weaknesses. Limited cyber war of this kind could be designed to slow an adversary's preparations for military intervention, as part of an economic warfare campaign, or as part of the manoeuvring that typically accompanies a crisis or confrontation between states.

More serious, and perhaps more likely, than limited cyber war is what can be termed unrestricted cyber war, a form of warfare that has three major characteristics. First, it is comprehensive in scope and target coverage with no distinctions between military and civilian targets or between the home front and the fighting front. Second, unrestricted cyber war has physical consequences and casualties, some of which would result from attacks deliberately intended to create mayhem and destruction, and some of which would result from the erosion of what might be termed civilian command and control capabilities in areas such as air-traffic control, emergency-service management, water-resource management and power generation. Third, the economic and social impact — in addition to the loss of life — could be profound.

An unrestricted cyber campaign would almost certainly be directed primarily against the target country's critical national infrastructure: energy, transportation, finance, water, communications, emergency services and the information infrastructure itself. It would likely cross boundaries between government and private sectors, and, if sophisticated and coordinated, would have both immediate impact and delayed consequences. Ultimately, an unrestricted cyber attack would likely result in significant loss of life, as well as economic and social degradation.

Denial-of-service attacks would take on new meaning where the services do not simply provide access to the internet but are systems supporting critical, national infrastructures; systems that are not designed for prolonged outages. A chronic loss of power generation and transmission capabilities, for example, would have a major impact on medical and other emergency services, communications capabilities and the capacity to manage. A failure of emergency services in major cities would not only result in the

deaths of those requiring such services but also in a loss of confidence in the government's ability to provide basic services and protection. As it became apparent that the attack was impacting other infrastructure such as communications, transportation and water, the levels of fear and loss of confidence would begin to impact the basic social fabric. Attacks against the financial infrastructure would erode the capacity of business to function normally and raise questions among the public about the security of their personal finances, including retirement accounts, investments and personal savings. Military networks, all of which utilise commercial communications pathways, would also be hampered, undermining command and control, logistics and both preparedness and operations. In unrestricted cyber warfare, virtual attacks can have consequences that are real, profound and far-reaching.

The irony is that those nations, like the United States and its NATO Allies, that have the capacity to excel in cyber war as an adjunct to military operations — and can achieve information dominance over the battlefield — are also those most vulnerable to unrestricted cyber war. There are, however, measures that can be taken to reduce these vulnerabilities.

Cyber warfare is not fundamentally different from conventional, physical warfare. When conducted by a nation state, it is integrated into a defined strategy and doctrine, becomes part of military planning and is implemented within specific parameters. Consequently, it is subject to analysis and warning in much the same way as other military operations. Indeed, there are several ways of reducing vulnerability to cyber war. These include anticipation and assessment, preventive or deterrent measures, defensive measures and measures for damage mitigation and reconstitution.

The Clausewitzian notion that war is an extension of politics by other means provides the basis for the development and implementation of a reliable warning system for cyber threat. Prior to an attack, whether cyber or conventional, there is usually an element of political confrontation. Awareness of an escalating political conflict, recognition and analysis of developing cyber-warfare capabilities, and detection and assessment of attack precursors all provide warnings of impending cyber attacks. While still being developed, methodologies to provide warning can be combined with coordinated and sophisticated survivability strategies to increase the likelihood of recognition, response and recovery from a concerted cyber attack.

Warning methodologies are all the more important because of the difficulties inherent in identifying and assessing a sophisticated cyber attack. Differentiating a network attack from accidental factors (such as a surge in demand for certain information on the network) or implementation mistakes (such as errors in the portion of a server's operating system that processes network traffic) is neither quick nor easy. Moreover, even when it is clear that an attack is underway, the defender must correlate multiple pieces of information (each of doubtful quality) to gain a better understanding of the actions involved in the attack, before deciding how best to respond. The degradation of network service, data quality or capacity makes this difficult, especially if the data on the network cannot be trusted.

Preventive or deterrent measures are difficult in the cyber world, partly because of the ability of attackers to remain anonymous. An unrestricted cyber-war offensive, however, would almost certainly provide some clues as to their identity. One of the issues for decision-makers in NATO countries for the future will therefore be whether such attacks lead simply to cyber retaliation or to retaliatory actions in the physical world, or both. Notions of linkage, escalation and deterrence that were familiar during the Cold War have to be re-examined in relation to new kinds of contingencies. Indeed, it might be that strategies of deterrence could have an impact in cyber space — at least against unrestricted offensives.

Defences can also be developed with some expectation of success. In the near term, modern network attack almost always favours the aggressor. In the long term, this advantage may shift to the defenders, as they identify the means of attack and block them by patching vulnerabilities and insulating network connections. Moreover, information networks can be made more robust. Essential network services can be isolated in order to maintain mission capability. Physical security and personnel training can minimise the threat of malicious insider activity. And firewalls and intrusion detection systems can be configured in such a way as to provide warning and response systems for both public and private infrastructures.

Finally, it is necessary to develop a capacity for damage mitigation and reconstitution. Network design should integrate notions of robustness and survivability (based in part on the availability of other means to perform critical missions), while contingency plans for the continued implementation of critical roles and missions with far less cyber connectivity are essential. Insulated intranets that can operate efficiently and safely without wider connections offer considerable promise in this respect.

All this is, of course, easier said than done. The obstacles to enhanced network survivability are many and varied. Security is often an afterthought rather than an integral part of network design. Government and business have different approaches to security and its provision. Dependence on computer networks often goes unquestioned. And the lines of responsibility in government are often blurred and confused by overlapping and competing jurisdictions. Yet all these difficulties can be overcome with a mixture of political will, organisational commitment, careful planning and systematic implementation. Defence planning needs to incorporate the virtual world, if there is to be any chance of limiting physical damage in the real world. ■