STRATEGIC INSIGHTS

ASPI

# Cyberspace and armed forces

## The rationale for offensive cyber capabilities

106

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

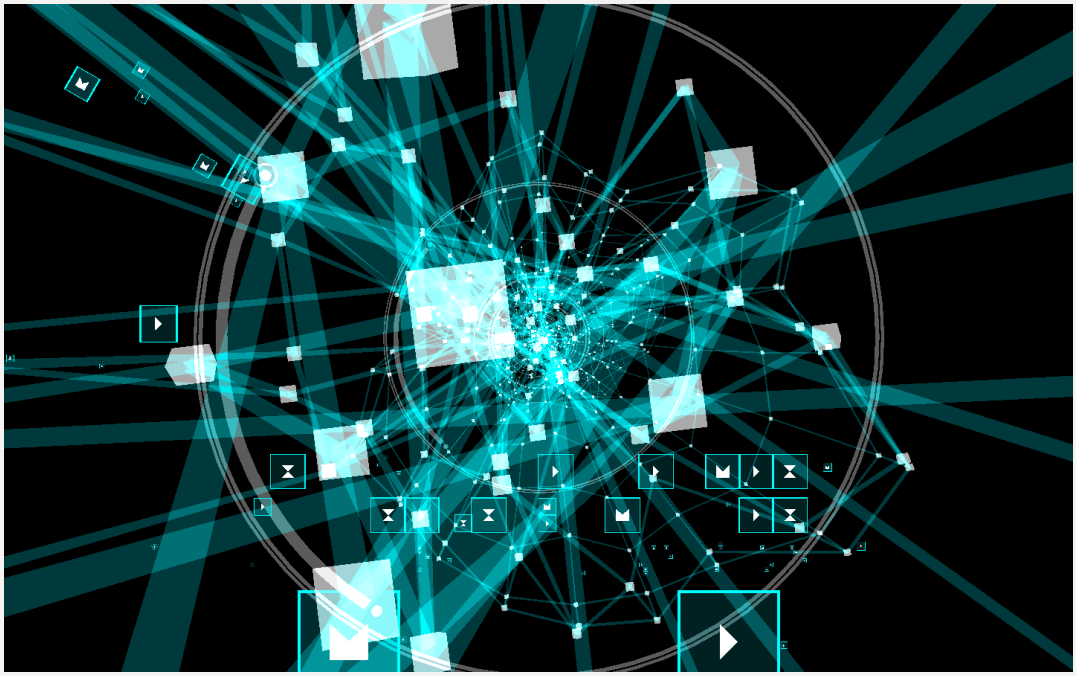
**James A Lewis**

An earlier version of this paper was originally prepared for a September 2015 workshop held by the German Ministry of Defense as part of its Weissbuch consultation.

### The need for cyber capabilities

A serious approach to military modernisation requires countries to equip, train, and organise cyberforces for what has become an essential component of national defence and deterrence. A force without adequate cyber capabilities is more dangerous to itself than to its opponents. As nations move forward in rethinking the role and nature of their military forces, and as they study the problems of organisation, doctrine and use of cyber operations, they need to:

- develop the full range of military cyber capabilities with both offensive and defensive application
- create a centralised command structure for those capabilities, with clear requirements for political-level approval for action
- embed those capabilities in doctrine and a legal framework based on international law.



The Defense Advanced Research Projects Agency's Plan X program is working to help military cyber operators visualise the cyber battlespace and perform missions there. DARPA photo, courtesy US Department of Defense.

Given the central importance of software and networks to effective military operations, renouncing offensive cyber capabilities is in effect a kind of unilateral disarmament. This may be appealing to some, perhaps, but it's irresponsible for those who seek to ensure their country's defence. The failure to develop 'offensive' capabilities condemns a nation to obsolete technology, outdated forces and inadequate defences. Nor is it desirable to leave cyber capabilities spread piecemeal across many units with disparate skills, missions and doctrines.

## What do offensive cyber operations entail?

Political concerns over offensive cyber capabilities have complicated discussions about whether to create and how to organise those capabilities. In fact, advanced military cyber capabilities can be used for either offensive or defensive purposes, just as is the case for any other class of weapon. Some of the concern about offensive cyber capabilities comes from the overestimation of effect prevalent in much of the literature on cyberwarfare. A clearer understanding of the military use of cyberattack helps make clear that creating cyber capabilities or organising to use them effectively isn't inherently contrary to international law; nor does it create new risks to peace.

There has been only a handful of incidents that we could consider an 'armed attack' or 'the use of force'. This lack of experience makes it easy to overestimate the military application of cyber capabilities, their effects, and their risks. Cyberattacks are a 'support weapon' that can shape the battlefield, but their ability to cause casualties or physical damage is very limited. Cyberattacks have produced physical destruction in only two instances. In no instances have there been any casualties. The remaining few attacks involved the disruption of data and networks or the manipulation of opponents' decision-making. Cyberattacks by themselves can't win a war, and the idea of 'cyberwar', a war waged solely with computer attacks, is ridiculous, because no country could expect cyberattacks by themselves to compel a reasonably motivated opponent to surrender.

Most cyberattacks will produce intangible effects. Expanding the 'fog of war' creates indecision and slows opponents' reactions in ways that confer military advantage. Modern weapons depend on software, and disrupting that software can damage their performance. Manipulating public opinion to damage an opponent's legitimacy and authority among both domestic and international audiences is also an objective we can expect some likely opponents to pursue. Some actions may provide only symbolic effects aimed at an attacker's domestic audience, but this too can be valuable. The ability to disrupt an attacker's networks, weapons, command and politics can provide significant advantage in combination with other weapons.

A number of hypothetical examples illustrate military effect. Air defence systems are most effective when they are networked. In addition, the individual components of those networks (radars, targeting computers, missiles) all depend on software for efficient operation. Interfering with networks or software would make air defences less effective. Militaries, like commercial companies, rely on computer networks for logistics. Interfering with logistics networks could result in shipments being cancelled or supplies being sent to the wrong places. Commanders rely on a flow of information from sensors and intelligence assets to determine the location, movement, and intentions of an opponent. Suddenly cutting off that information or introducing deliberate inaccuracies could have a paralysing effect. The introduction of false information into command networks increases the likelihood of tactical errors—troops are sent to the wrong location, fire on each other or are lured into ambushes.

These are not 'kinetic effects' similar to the blast created by traditional weapons using explosives and projectiles. Most of the result of a cyberattack will be to create intangible (as opposed to physical), non-kinetic effects that create confusion, shape opinion and disrupt data or services. Cyberweapons can in some circumstance cause physical damage, but those effects require very advanced skills, are time-consuming to produce and may provide only limited military benefit.

There are of course some classes of weapons whose use the international community has rejected because of their horrific effect or the potential for unconstrained harm to civilian targets. They are primarily weapons of mass destruction (with an implicit but powerful constraint on the use of nuclear weapons) and a few other military technologies, such as cluster munitions and some forms of land mines that create indiscriminate effect. Cyberattack does not fall into these categories because of its limited physical effect and because the most damaging attacks must be precisely designed, limiting the risk of indiscriminate effect.

Civilian infrastructure is a legitimate target in wartime, subject of course to the constraints and principles of international law. However, military planners now often seek to avoid damage to civilian infrastructure. The benefits of such damage are limited in short conflicts, the effect on world opinion may outweigh the gains and, in some cases, the disruption of civilian infrastructure won't degrade the performance of the defender's forces quickly enough to provide military advantage. Temporary and reversible disruption of services through cyberattack is a more likely outcome than infrastructure destruction.

A decision to focus on military networks as targets reduces the risk of collateral damage (hospitals are unlikely to be on the same computer network as air defence systems) and reduces the chance that an attack on a legitimate military target will spill over and harm innocent civilians. The one area where civilian infrastructure could provide an attractive target for cyberattacks is electrical power generation and transmission, since militaries depend to some degree on civilian electrical infrastructure. Having the ability to attack civilian infrastructure, however, does not mean a nation can choose to do so. As with any weapon, how a nation decides to use it will constrain unwanted effect. In general, damaging civilian targets through cyberattack is less useful than attacks on weapons, sensors, or command and control.

This isn't an arms race—our strategic dialogue would benefit from restraint in citing antique precedents from the Cold War. The most likely opponents we face have already developed offensive cyber capabilities, whether they admit to them in public or not. If anything, it's this lack of transparency that's destabilising. The acquisition of an ability to operate in cyberspace is best seen as a step in military modernisation necessary to maintain the value of existing investments in weapons and forces.

It's worth considering the linkage between cyberwarfare and electronic warfare (EW), which was the first of the intangible spheres of combat. EW interferes with the communications and sensors that support operations, including the targeting of opponents' weapons. EW and cyber capabilities are merging but, unlike EW, which tends to take relatively static forms, a cyber capability is dynamic and requires greater control and management to allow for rapid change and adjustment if it is to retain its effectiveness. An aircraft, armoured unit or ship that lacks EW capabilities is essentially a target, and a failure to move ahead with military cyber capabilities will do increasing and perhaps fatal damage to any nation's ability to operate in combat against a modern opponent.

## Control of offensive cyber capabilities

Whether the creation of cyber capabilities is dangerous to peace or destabilising is a matter of choice. They are not inherently offensive. It's the policies that guide their use that determine whether their acquisition is offensive. States that are attracted to the use of coercive techniques to achieve their foreign policy goals will find cyberattack a useful addition to their arsenal. States with a defensive orientation and a commitment to the peaceful resolution of international disputes won't find either changed by the acquisition of offensive cyber capabilities.

While there's no international agreement on what cyber actions qualify as an attack or the use of force, there's implicit international understanding that a cyber action that produces an effect equivalent to an attack using conventional weapons and produces physical destruction or casualties would be considered as the use of force or an armed attack. These terms come from Articles 2/4 and 51 of the UN Charter, and reaching shared international understandings on them is essential for the application of international law. Deciding on the national level—through policy, law and military doctrine—what qualifies as the use of force or an attack is essential for ensuring that military cyber actions are conducted in a manner consistent with international humanitarian law. For the purposes of this discussion, we can consider a cyberattack to be an action undertaken to achieve military effect.

However, a range of coercive actions fall below this 'use of force / armed attack' threshold, the same way that sending military aircraft to prowl along the borders of national airspace can be threatening and intended to coerce, but isn't an attack. Such grey areas create complex problems for the application of international law and for defence policy. These problems can be addressed at least in part by drawing upon precedents from the physical world. Cyber incidents of sufficient scope, intensity and duration to create harmful consequences with significant scale and immediate effect could be considered an armed attack, but in this grey area in international law this is a decision that only a nation's political leadership can make.

Clear guidelines on use, consistent with international humanitarian law, make cyber 'weapons' an intrinsic element of national defence, rather than a troubling expansion of offensive capabilities. In this regard, the recently concluded 2015 UN Group of Government Experts endorsed the applicability of fundamental guiding principles for armed conflict drawn from international law, including the principles of humanity, necessity, proportionality, and distinction. These principles form the core of the laws of armed conflict; agreement to observe them in the use of military operations in cyberspace makes cyberattack the equivalent of other types of weapons whose use is constrained but not forbidden.

The risk of collateral damage can also be reduced and mitigated by creating careful command and control structures for cyber operations and assets, and by ensuring that operations that entail political risk require senior-level political authorisation (in the US, for example, offensive cyber operations require presidential approval). Until nations gain more experience and until the technology matures, a clear chain of command reaching to the political level of authorisation is best. As with any weapon, policy and doctrine allow nations to control use and risk.

## Creating a cybercommand

If a nation's military forces are not to become a museum display, they must acquire and organise cyberattack capabilities. How to organise these new capabilities was an open question a few years ago, but nations are now increasingly centralising their military cyber assets into some kind of 'cybercommand'—a single military unit that integrates their existing cyber capabilities into a more coherent whole. This move has implications for workforce development, doctrine and the integration of cyberattack into planning and operations with other units and combat arms.

When the US created its Cyber Command, the original intent was defensive, to centralise resources and ensure better coordination among defensive elements. Creating a cybercommand provides several benefits. First, it enhances coordination, improves defensive capabilities and allows defensive and offensive action to be more easily 'deconflicted'. Second, it makes the acquisition of cyberattack tools and training easier and less expensive (and the training burden shouldn't be underestimated). While cyber capabilities need to be integrated into existing land, air and naval forces, cyberspace is a global 'domain' and a specialised command improves the ability to defend that domain and to engage in 'strategic' operations (for example, those not aimed at immediate battlefield effect).

Military use of cyber techniques is not the same as espionage, although attack and spying are related (at least in their initial phases), and target reconnaissance is critical for cyber operations. Cyber action to collect intelligence of value to military operations is vital and legitimate, but it isn't attack. While the skills and tools are similar, an easy distinction is that intelligence supports decision-making while attacks interfere with decision-making. The most important area of overlap between cyber espionage and cyberattack is the need to ensure that espionage on networks is coordinated with military cyber operations to avoid 'fratricide', so that they do not disrupt each other; in this, having a centralised command can be invaluable.

Restricting military cyber operations and capabilities to the purely defensive cedes the initiative to the opponent. It forces the defender into a reactive posture, both strategically and tactically. Counterintuitively, better cyber defence requires knowledge of offensive capabilities. Defence can learn from offence in ways that strengthen security, and offensive capabilities provide the ability to detect and disrupt attacks before they do damage.

The conventional approach to defensive cyber operations has been to focus on technical rather than strategic solutions. An orthodox network defence, limited to reactive activities on the defender's own networks, accentuates what's essentially a point defence approach. This reflects a time when networks were an administration support tool rather than the operational environment they have become. It may be that this 'fire department' approach of rushing from crisis to crisis to put out fires and restore services is politically desirable, but it ensures that the defender will always be one or more steps behind the attacker and it limits policymakers' options for response in unhelpful ways. Arguments that limiting cyber capabilities to the defensive has a deterrent effect rely on a sequence of improbable events and assumptions about attackers' intentions and perceptions.

Military cyber capabilities will become a crucial part of alliance commitments. NATO is wrestling with the question of moving from a purely defensive technical stance to doctrine that incorporates offensive capabilities into alliance forces and planning in some way. In the light of heightened tensions and new kinds of conflict (sometimes called 'hybrid' warfare), it's hard to see how NATO can maintain a credible deterrent force without possessing the full range of cyber capabilities, both offensive and defensive. No-one would argue that NATO should confine itself to air defence systems and abjure fighter aircraft, and the same is true for cyber capabilities. The acquisition by NATO of cyberattack capabilities (called 'active defence' in NATO parlance) will oblige the alliance to define new requirements. Command and authorisation authorities for cyberattack must be explicitly stated and part of regular planning, exercises and consultation. Those same requirements apply to national cyber capabilities.

Advances in technology have continuously changed the nature of warfare since the onset of the Industrial Revolution. The adoption of cyber techniques for military use is the latest phase in this long history of change and adaptation. Offensive cyber capabilities make for better defences, even if they are never used. No rational person wishes for war, and Western militaries today are intended to deter attack, but to do so effectively they must acquire effective cyberattack capabilities. As Roman strategists said long ago, 'If you want peace, prepare for war.'

## Acronyms and abbreviations

EW electronic warfare

NATO North Atlantic Treaty Organization

## Important disclaimer



## About the author

**Dr James A Lewis** is an ASPI-ICPC International Fellow. He is a senior fellow and director of the Technology and Public Policy Program at CSIS, where he writes on technology, security, and the international economy.

## About Strategic Insights

Strategic Insights are shorter studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

## ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.thestrategist.com.au

Facebook.com/ASPI.org

@ASPI_org