Hype and fear

America is leading the way in developing doctrines for cyber-warfare. Other countries may follow, but the value of offensive capabilities is overrated

Even as anxiety about jihadi terrorist threats has eased, thanks to the efforts of intelligence agencies and drone attacks' disruption of the militants' sanctuaries, fears over Western societies' vulnerability to cyber-assaults have grown. Political and military leaders miss no chance to declare that cyberwar is already upon us. America's defence secretary, Leon Panetta, talks of a "cyber-Pearl Harbour". A senior official says privately that a cyber-attack on America that "would make 9/11 look like a tea party" is only a matter of time.

The nightmares are of mouseclicks exploding fuel refineries, frying power grids or blinding air-traffic controllers. The reality is already of countless anonymous attacks on governments and businesses. These seek to disrupt out of malice, or to steal swathes of valuable commercial or security-related data. Some experts believe that such thefts have cost hundreds of billions of dollars in stolen R&D.

Many of these attacks are purely criminal. But the most sophisticated are more often the work of states, carried out either directly or by proxies. Attribution—detecting an enemy's fingerprints on a cyber-attack—is still tricky, so officials are reluctant to point the finger of blame publicly. But China is by far the most active transgressor. It employs thousands of gifted software engineers who systematically target technically advanced Fortune 100 companies. The other biggest offenders are Russia and, recently, Iran (the suspected source of the Shamoon virus that crippled thousands of computers at Saudi Arabia's Aramco and Qatar's RasGas in August).

America and its allies are by no means passive victims. Either America, Israel or the two working together almost certainly hatched the Stuxnet worm, found in 2010, that was designed to paralyse centrifuges at Iran's Natanz uranium-enrichment plant. The Flame virus, identified by Russian and Hungarian experts this year, apparently came from the same source. It was designed to strike at Iran by infecting computers in its oil ministry and at targets in the West Bank, Syria and Sudan.

Boring, not lurid

For all the hype, policies on cyber-warfare remain confused and secretive. The American government is bringing in new rules and a clearer strategy for dealing with cyber-threats.

Barack Obama is said to have signed in October a still-secret directive containing new guidelines for federal agencies carrying out cyber-operations. It sets out how they should help private firms, particularly those responsible for critical national infrastructure, to defend themselves against cyber-threats by sharing information and setting standards.

The directive is partly a response to the stalling of cyber-legislation in the Senate. Republican senators argue that it imposes too great a regulatory burden on industry, which is already obliged to disclose when it is subject to a cyber-attack. It is also meant to govern how far such bodies as the Department of Homeland Security can go in their defence of domestic networks against malware attacks.

The Pentagon is also working on more permissive rules of engagement for offensive cyber-warfare, for example to close down a foreign server from which an attack was thought to be emanating. General Keith Alexander heads both Cyber Command (which has a budget of $3.4 billion for next year) and the National Security Agency. He has often called for greater flexibility in taking the attack to the "enemy". The emergence of new cyber-warfare doctrines in America is being watched closely by allies who may follow where America leads—as well as by potential adversaries.

However, Jarno Limnell of Stonesoft, a big computer security firm, says that all levels of government in the West lack strategic understanding on cyber-warfare. So, although questions abound, answers are few. For example, it is not clear how much sensitive information about threats or vulnerabilities government agencies should share even with private-sector firms that are crucial to national security. Often the weakest link is their professional advisers, such as law firms or bankers who have access to sensitive data.

Almost all (roughly 98%) of the vulnerabilities in commonly used computer programmes that hackers exploit are in software created in America. Making private-sector companies more secure might involve a controversial degree of intrusion by government agencies, for example the permanent monitoring of e-mail traffic to make sure that every employee is sticking to security rules. Government hackers may also like to hoard such vulnerabilities rather than expose them. That way they can later create "backdoors" in the software for offensive purposes.

Also controversial is the balance between defence and attack. General Alexander stresses that in cyber-warfare, the attacker has the advantage. Mr Limnell says that, although America has better offensive cyber-capabilities than almost anybody, its defences get only three out of ten.

Setting rules for offensive cyber-warfare is exceptionally tricky. When it comes to real, physical war, the capability may become as important as air superiority has been for the past 70 years: though it cannot alone bring victory, you probably can't win if the other side has it.

China has long regarded the network-centric warfare that was developed by America in the late-1980s and copied by its allies as a weakness it might target, particularly as military networks share many of the same underpinnings as their civilian equivalents. The People's Liberation Army (PLA) talks about "informationisation" in war, "weakening the information superiority of the enemy and operational effectiveness of the enemy's computer equipment". China's planning assumes an opening salvo of attacks on the enemy's information centres by cyber, electronic and kinetic means to create blind spots that its armed forces would then be able to exploit. Yet as the PLA comes to rely more on its own information networks it will no longer enjoy an asymmetric advantage. Few doubt the importance of being able to defend your own military networks from cyber-attacks (and to operate effectively when under attack), while threatening those of your adversaries.

But to conclude that future wars will be conducted largely in cyberspace is an exaggeration. Martin Libicki of the RAND Corporation, a think-tank, argues that with some exceptions cyber-warfare neither directly harms people nor destroys equipment. At best it "can confuse and frustrate…and then only temporarily". In short, "cyber-warfare can only be a support function" for other forms of war.

Four horsemen

Besides the cyber element of physical warfare, four other worries are: strategic cyberwar (direct attacks on an enemy's civilian infrastructure); cyber-espionage; cyber-disruption, such as the distributed denial-of-service attacks that briefly overwhelmed Estonian state, banking and media websites in 2007; and cyber-terrorism. Gauging an appropriate response to each of these is hard. Mr Limnell calls for a "triad" of capabilities: resilience under severe attack; reasonable assurance of attribution so that attackers cannot assume anonymity; and the means to hit back hard enough to deter an unprovoked attack.

Few would argue against improving resilience, particularly of critical national infrastructure such as power grids, sewerage and transport systems. But such targets are not as vulnerable as is now often suggested. Cyber-attacks on physical assets are most likely to use what Mr Libicki calls "one-shot weapons" aimed at industrial control systems. Stuxnet was an example: it destroyed perhaps a tenth of the Iranian centrifuges at Natanz and delayed some uranium enrichment for a few months, but the vulnerabilities it exposed were soon repaired. Its limited and fleeting success will also have led Iran to take measures to hinder future attacks. If that is the best that two first-rate cyber-powers can do against a third-rate industrial power, notes Mr Libicki, it puts into perspective the more alarmist predictions of impending cyber-attacks on infrastructure in the West.

Moreover, anyone contemplating a cyber-attack on physical infrastructure has little idea how much actual damage it will cause, and if people will die. They cannot know if they are crossing an adversary's red line and in doing so would trigger a violent "kinetic" response (involving real weapons). Whether or not America has effective cyber-weapons, it has more than enough conventional ones to make any potential aggressor think twice.

For that reason, improving attribution of cyber-attacks is a high priority. Nigel Inkster, a former British intelligence officer now at the International Institute for Strategic Studies, highlights the huge risk to the perpetrator of carrying out an infrastructure attack given the consequences if it is detected. In October Mr Panetta said that "potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests."

He may be over-claiming. Given that cyber-attacks can be launched from almost anywhere, attribution is likely to remain tricky and to rely on context, motive and an assessment of capabilities as much as technology. That is one reason why countries on the receiving end of cyber attacks want to respond in kind—ambiguity cuts both ways. But poor or authoritarian countries attacking rich democratic ones may not have the sorts of assets that are vulnerable to a retaliatory cyber-attack.

The difficulty is even greater when it comes to the theft (or "exfiltration", as it is known) of data. For China and Russia, ransacking Western firms for high-tech research and other intellectual property is tempting. The other way round offers thinner pickings. In 2009 hackers from an unnamed "foreign intelligence agency" made off with some 24,000 confidential files from Lockheed Martin, a big American defence contractor. As a result they could eavesdrop on online meetings and technical discussions, and gather information about the sensors, computer systems and "stealth" technology of the F-35 Joint Strike Fighter. This may have added to the delays of an already troubled programme as engineers tried to fix vulnerabilities that had been exposed in the plane's design. Investigators traced the penetrations with a "high level of certainty" to known Chinese IP addresses and digital fingerprints that had been used for attacks in the past. Less than two years later, China unveiled its first stealth fighter, the J-20.

Theft from thieves

As Mr Libicki asks, "what can we do back to a China that is stealing our data?" Espionage is carried out by both sides and is traditionally not regarded as an act of war. But the massive theft of data and the speed with which it can be exploited is something new. Responding with violence would be disproportionate, which leaves diplomacy and sanctions. But America and China have many other big items on their agenda, while trade is a very blunt instrument. It may be possible to identify products that China exports which compete only because of stolen data, but it would be hard and could risk a trade war that would damage both sides.

Cyber-disruption has nuisance value and may be costly to repair, but it can be mitigated by decent defences. Cyber-terrorism has remained largely in the imagination of film-makers, but would be worth worrying about if it became a reality. Stonesoft's Mr Limnell reckons that,

though al-Qaeda and its offshoots show little sign of acquiring the necessary skills, they could buy them. Mr Libicki is more sceptical. Big teams of highly qualified people are needed to produce Stuxnet-type effects, which may be beyond even sophisticated terrorist groups. Also, the larger the team that is needed, the more likely it is to be penetrated.

The Obama administration's attempt to develop a more coherent—and perhaps less secret—doctrine of cyber-warfare is sensible so long as it is not just an excuse for hyping something that, as far as is known, has yet to kill anybody. The idea that offence beats defence is also suspect. If more attention were paid to fixing the security flaws in Western software, cyber-attackers would have fewer entry points. And more effort should be put into solving the attribution problem. Getting caught is a deterrent that state actors take seriously. But given that the essence of cyber-warfare is ambiguity and uncertainty, gaining clarity and certainty will be exceptionally difficult. That makes policy both hard to construct and harder still to explain.

Fonte: The Economist, London, v. 405, n. 8814, p. 62-63, 8 a 14 Dec. 2012.