S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 198/2012 dated 23 October 2012

Cyberattacks in the Gulf: Lessons for Active Defence

By Damien D. Cheong

Synopsis

The recent cyberattacks on two oil and gas corporations in the Gulf raises the question of whether countries should rely on active defence in the absence of international laws governing the behaviour of states in cyberspace.

Commentary

THE SAUDI Arabian state-owned oil company Aramco and the Qatari natural gas producer RasGas were victims of a major cyberattack in August 2012. A computer virus known as Shamoon penetrated the systems of both companies and reportedly disabled over 30,000 computers. US Defence Secretary, Leon Panetta, has called the attacks "the most destructive the private sector has seen to date".

Preliminary investigations by the US have suggested that the hackers were either Iranian-sponsored or were closely aligned with Tehran. Iran has denied the allegations, and offered to assist with the on-going investigations to "find the source of the attacks".

Targeting the Private Sector

The cyberattacks on Aramco and RasGas were not only tactical but strategic as well. Attacking a private sector company can be easier than attacking a military and/or prominent government organisation (although hackers have not shied away from attempting to attack the latter). This is because private sector companies often have inadequate security protocol; make little investment to secure cyber infrastructure; need to deal with legislative stumbling blocks; possess a general lack of awareness about the seriousness of cyberthreats; and have misperceptions about their vulnerabilities, which make them soft targets for hackers.

Arguably, the most important factor that renders a system vulnerable, whether in the private or public sector, is the human factor. In the Aramco and RasGas incidents, a Reuters report suggests that as Aramco's security systems were adequate at the time of the attack, the hackers must have obtained insider assistance.

Private sector companies are increasingly operating critical infrastructure like electrical grids and telecommunications, as well as providing essential supplies like oil, gas and even water. Hence strategically, an attack on or theft of confidential data from such companies could seriously undermine a country's national security. As suspected in the Aramco and RasGas cases, motivations for cyberattacks are not limited to

industrial espionage and mischief-making, but may actually involve political and strategic objectives as well.

Since states first began recognising the significance of cyberthreats to national security, there has been a push for the development of universally-acceptable legislation to regulate state behaviour in cyberspace. However, despite much debate, it has been difficult to get consensus on the terms of the legislation as well as the major issues such as enforceability, accurate attribution and sovereignty.

In addition, many states are not keen to sign such legislation as they fear it would significantly undermine their strategic options, and put them at a severe disadvantage against more technologically-advanced states. As a result, states may not have legal recourse if attacked, and may be compelled to adopt unilateral measures to protect themselves.

Unilateral measures against cyberthreats

The first option, proposed by the US last year, is the use of a kinetic or 'hard power' response to major cyberattacks. A major attack is one that attempts to disrupt critical infrastructure or causes significant damage and/or casualties. In light of the seemingly ungovernable nature of cyberspace, this response is designed to intimidate and discourage potential hackers and states from perpetrating cyberattacks.

However, the difficulties of attribution, in addition to the diplomatic fallout and significant economic costs, suggest that this option should only be used as a last resort. Moreover, if more countries adopt this approach, a new type of global lawlessness would invariably ensue.

The second option, although highly controversial, is active defence. Active defence is formally defined by the US Department of Defence (DoD) as its "synchronised, real-time capability to discover, detect, analyse, and mitigate threats and vulnerabilities…It operates at network speed using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems". Put simply, active defence is "the use of offensive cyberactions, such as counter hacking or pre-emptive hacking" against the perpetrator of the cyberattack.

It involves: "(a) detecting an intrusion; (b) tracing the intruder; and (c) some form of cyber counter strike". The main advantages of active defence are that it can delay, deceive, deny, distract and most importantly, deter hackers. Active defence is not limited to the public sector but can and indeed has been employed by private sector entities as well. It seems that active defence would be the most viable at this point in time since it is covert and it minimises and/or eliminates much of the diplomatic fallout.

Government and private sector cooperation

The above-mentioned approaches notwithstanding, it is extremely crucial to bolster cybersecurity in the private sector. The Singapore government has acknowledged that "no one person, company or government agency can ensure Singapore's cybersecurity on its own"; hence it has expressed its willingness to work closely with the private sector in dealing with cyberthreats.

As part of its Infocomm Security Masterplan 2, the government will harden national infocomm infrastructure and services; enhance infocomm security competencies; cultivate vibrant infocomm security ecosystem; and increase international collaboration. Private sector collaborations, in the government's view, are crucial in enhancing infocomm security competencies and cultivating a vibrant infocomm security ecosystem.The government has also suggested that private sector companies adequately train and educate their employees in the prevention, detection and response to a cyberattack; update and test their systems regularly to ensure they are up-to-date; and make cybersecurity a top management priority and plan for future contingencies and exigencies that relate to cyber.

The cyberattacks on Aramco and RasGas highlight the imperative for states to rapidly develop global legislation through international organisations like the UN to regulate cyberspace. However, until such legislation is in place and is capable of being enforced, cyberdefence will be unilateral. In this context, active defence, while controversial, is an approach that should be carefully explored.

Damien D. Cheong is a Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.