NEW STRAITS TIMES

Tuesday, January 20, 2015

Are cyber attacks 'acts of war'?

By Elina Noor

NO GUIDELINES: *There are questions on what recourse is available to states, and what the international legal framework should govern*

IN the aftermath of the Paris attacks of Jan 7-9, as people all over the world were debating whether they were Charlie, Ahmed some other nominal symbol, a different kind of exchange was taking place in cyberspace. Anonymous, the collective hacking legion, launched #OpCharlieHebdo targeting specific websites in reaction to the attacks and in defence of the freedom of expression.

A few days later, the French government reported attacks against some 20,000 websites, a number of them belonging to French media. These were done presumably in response to the solidarity march on the streets of Paris. For many of these sites, service was restored within a few hours, no real damage had been inflicted, and no nation-state appeared to have been involved in any of these attacks.

However, if any of these details had been different, how might the French or any government in its situation have responded? Contrast these multiple cyber attacks to the Sony hack late last year. Contrast also the resulting pandemonium from the latter and consider how, why, and whether the two should be treated differently.

The Sony hack leaked an embarrassing trove of confidential personnel information, company communication, and unreleased movies. Yet despite the threat of violence by the perpetrators, the "Guardians of Peace", no actual death or destruction resulted. Like the terror attacks in Paris, the United States government, the entertainment industry, and many others saw the Sony hack which initially compelled the scrapping of, *The Interview* as an attack against free speech. Some, like Senator John McCain, went further to conflate the hack as probably "the greatest blow to free speech in (his) lifetime" with an "act of war" that demanded a response in kind.

Despite Sony's size (its 2013 total revenue of nearly seven trillion yen (about RM213b) dwarves the defence budget of many small countries), a hack into its computer system, while a cyber insecurity expose and a public relations nightmare, was not an attack against national critical infrastructure by any stretch of the imagination. If anything, it was as President Barack Obama called it: “cyber vandalism".

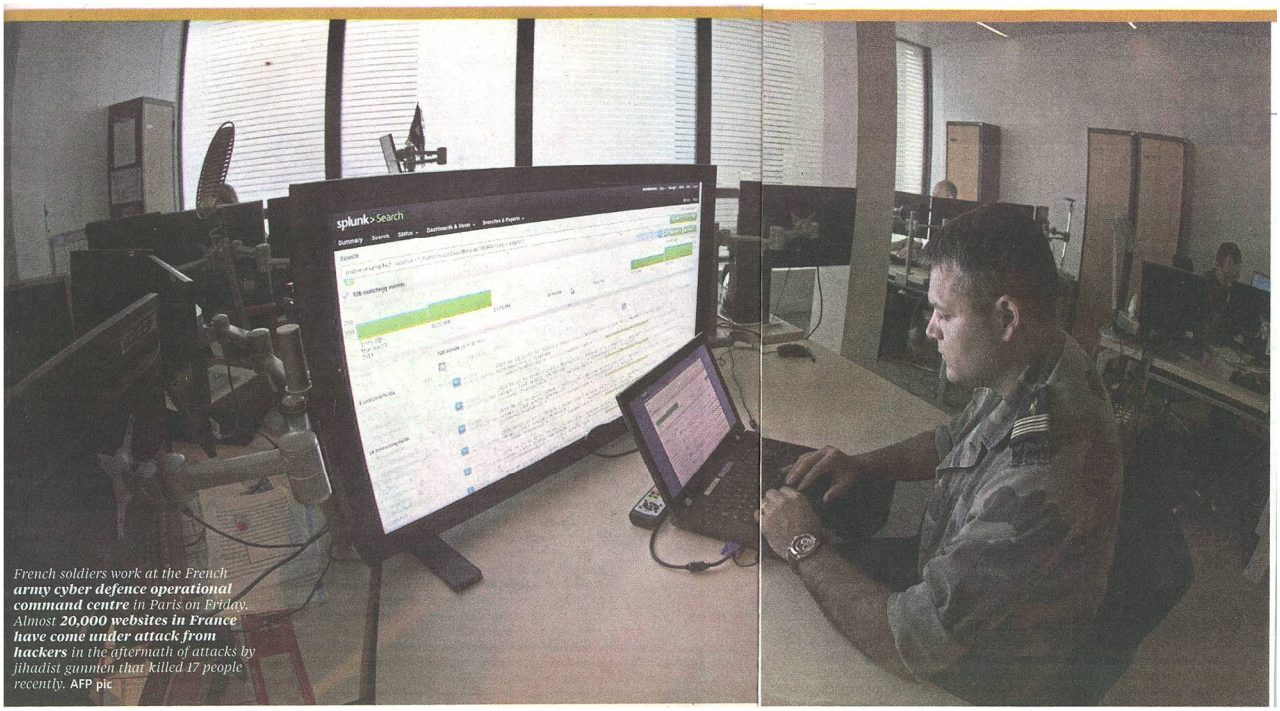
There were domestic political reasons in the US, of course, that coloured calls of a cyber war but the incident begs the more pressing, nebulous questions of when a cyber attack may in fact amount to an act of war, what recourse is available to nation states, and what international legal framework should govern.

There is the argument that a cyber attack can never constitute an act of war or an armed attack unless it fulfils the classical definition of war: there must be violence employed to compel submission by the opponent.

The qualification is an important one. It sets a high threshold for a legal response within the scope of the United Nations (UN) Charter which allows states to invoke self-defence measures under Article 51.

The rejoinder is that even if cyber attacks do not end up causing violent harm or destruction, they can in these and evolving times still bring a state to its knees by incapacitating its critical systems and services, particularly if they are extensively connected. For many countries, the vulnerability is exacerbated because their civilian and military infrastructures both information and physical typically overlap.

This effects-based argument calls for a broader definition of the use of force which is regulated by both customary international law and treaty law of the UN Charter. Since international law does not define the parameters of the use of force, this approach also necessitates a rethinking of whether the term can be creatively interpreted to discount the requirement of violence by means of traditional



French soldiers work at the French ***army cyber defence operational command centre*** *in Paris on Friday. Almost* ***20,000 websites in France have come under attack from hackers*** *in the aftermath of attacks by jihadist gunmen that killed 17 people recently.* AFP pic

weapons. If so, it broaches the question of whether the use of force in cyber space could ever reach the level of an armed attack.

Disappointingly, the debate on this among states is playing out along predictable political and power fault lines. Even as the US, China, and Russia seek to clarify conduct in cyber space bilaterally among themselves, separately these and other major powers have surged ahead on different tracks.

While the US and North Atlantic Treaty Organisation (Nato) have concluded that hostile cyber attacks may trigger a response by force, China and Russia in 2011 opted for different tact and terminology in their joint proposal for an International Code of Conduct for Information Security.
If technology and cyber space are meant to level the playing field between the world's haves and have-nots, then countries in this and other developing regions may wish to - no, should - have a say in determining the threshold of the use of force in the cyber domain and formulating their own policy positions, accordingly.

Malaysia, as one of Southeast Asia's most mature ICT economies, Asean Chair of 2015, and UN Security Council non-permanent member for 2015-2016, has an exceptional window of opportunity to contribute thought-leadership in this for the region beginning this year.

Elina Noor is ISIS Malaysia Assistant Director, Foreign Policy and Security Studies