RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 012 – 21 January 2019

The Advent of "CyWar": Are We Ready?

By Kumar Ramakrishna

SYNOPSIS

The recent SingHealth hack and the fake news phenomenon are likely harbingers of an emergent inflection point in contemporary war: CyWar. The aim of CyWar is to secure command of a State's "hard" and "soft" cyberspace. It behooves States to be ready to cope with the rising CyWar challenge.

COMMENTARY

TWO STAFF members of the Integrated Health Information Systems (IHiS) were recently sacked for negligence that contributed to the large scale SingHealth cyberattack, which took place between 27 June and 4 July 2018. The hack resulted in the loss of the personal data of 1.5 million patients with the public healthcare group.

The year 2018 was incidentally, also the year of "fake news": the Select Committee on Deliberate Online Falsehoods deliberated the issue in March with 65 individuals and organisations and submitted its report in September, recommending measures such as enacting new laws, urging technology companies to better police their platforms and to more systematically guide public education on falsehoods nationally.

Blurred Lines of "CyWar"

At first glance, these two episodes may seem unrelated. At a higher, strategic level of analysis, however, both are arguably connected in this emerging era of what we may call *CyWar.* Classically, the 19th century Prussian war philosopher Clausewitz noted that "war is politics by other means". That is, war is an instrument of an Intervening State to impose its political will on a Target State, to change the latter's behaviour in ways that advance the interests of the former.

Traditionally, war in the form of conventional military firepower has been a means of last resort. The instruments of state power have represented a spectrum of influence, ranging from diplomacy, economic policy including sanctions, military force, and strategic information operations.

Since the 1990s, however, due to rapid advances in computing power and communication technology − in particular the rise of the Internet, cheap broadband access and inexpensive smartphones − we may have arguably reached an inflection point. Strategic information operations or more precisely, strategic *cyberspace* operations, may well be becoming the dominant instrument of state power.

CyWar's Transformational Impact

CyWar has been transformational in several ways. First, war need no longer be officially declared: many analysts for instance have identified China, Russia, Iran and North Korea as being involved in significant cyberattacks short of formal declarations of war.

Second, military force may not necessarily be needed to severely damage a Target State; as Russian cyberattacks in Estonia in 2007 and Ukraine since 2014 have shown, through cyberspace, the Intervening State can severely degrade Target State critical national infrastructural networks.

Third, CyWar no longer involves solely formal Intervening State organs. The Chinese military can tap upon thousands of so-called informal "patriotic hackers" to engage in cyberattacks against Target States; whilst the Russian intelligence services have even co-opted organised crime for their operations as well.

Fourth, there is not much of a firewall between a physical data hack and its wider psychological impact. When North Korean elements in late 2014 hacked Sony Pictures' confidential personnel database to deter the studio from releasing a comedy about a plot to kill its leader, what seemed at first to be a large data breach soon became something more insidious.

Shaken Sony Pictures employees were also threatened that if they did not speak out against their company they and their families would be harmed as well. The FBI had to reassure them of their safety. In short, in CyWar, the old lines have been blurred.

Securing "Hard" and "Soft" Cyberspace

CyWar behooves us to analyse seemingly disparate episodes in cyberspace, such as fake news and strategic database breaches, more strategically and holistically. For instance, what on the surface may seem at first to be a profit-oriented criminal hack of confidential personal information may possibly be part of a larger, longer term Intervening State-orchestrated campaign to systematically analyse the structural vulnerabilities of the Target State, with a view to dominating it politically downstream.

From the latter's perspective, nevertheless, mitigating strategies are possible. Target State public and private sector stakeholders must in essence develop a broader understanding of what amounts to "critical infrastructure" in the CyWar age. *This*

requires reframing cybersecurity as an exercise in building data, infrastructural and social resilience.

To achieve this, a very preliminary and generic strategic inventory comprising four critical questions is proffered below. Different Target State sectors, public and private, could consider adapting such an inventory to systematically develop strategies for securing "hard" cyberspace domains like proprietary data and essential services, as well as "soft" cyberspace spheres such as the social cohesion of multi-cultural communities, and trust between the State and Citizens:

Four Critical Questions

First, what specific data, essential services or shared value system are of critical importance in one's domain, which if compromised, would adversely impact one's ability to compete or function optimally?

Second, how are such data, essential services or shared value systems currently secured? Are the domain owners clearly identified and basic safeguards in place?

Third, what processes exist to ensure that CyWar attacks in the form of hacks to steal data, distributed denial of service attacks to disrupt essential services, or manipulated news to disrupt social cohesion and public trust, do not cause a systemic "crash"?

In CyWar, defensive measures alone are not enough. As mutual nuclear deterrence kept the Cold War from getting hot, national Target State capabilities to deter aggressive Intervening States are likewise needed to help protect Target State cyberspace. In this regard, fourth and finally, does the Target State possess realistic response options short of military force?

These can range from legal and diplomatic challenges, economic sanctions, to quietly credible cyber-offensive capabilities in coordination with friendly international partners, that potentially aggressive Intervening States have to take into account −− and may well encourage the latter to commit to more reasonable cyber behaviour in line with developing international norms.

Are We Ready?

The emerging CyWar era is not unprecedented. There have been similar inflection points in the past. While Clausewitz earned acclaim for explaining the new European age of destructive mass Napoleonic warfare in the early 19th century, a century later, nuclear strategists like Bernard Brodie arrived at the paradoxical analysis that the overriding value of atomic weapons was to certainly flaunt them but never ever use them.

There are now similar attempts by a newer generation of strategic analysts to come to grips with what has been variously called "LikeWar" and "Code War" – and now of course, CyWar. Eventually a widely accepted term will emerge. What matters more though is are we conceptually, technically and geopolitically ready to respond to the emerging Age of CyWar?

Kumar Ramakrishna is Associate Professor and Head of Policy Studies and Head of the National Security Studies Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg