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

RSIS COMMENTARY

www.rsis.edu.sg No. 103 – 22 May 2020

Global Health Security:
COVID-19 & Its Impacts

Cyber Attacks on Healthcare Systems: Infrastructure Protection Critical

By Eugene EG Tan

SYNOPSIS

Healthcare systems all over the world are being subject to attacks even as the fight against COVID-19 rages on. States need to take critical infrastructure protection – like healthcare systems – more seriously.

COMMENTARY

ON 16 APRIL 2020, Czech authorities warned its international allies of "imminent, large scale attacks on hospitals". They know the effects of such an operation. Brno University Hospital, the second largest hospital in Czech Republic, has had to reschedule operations, relocate patients, and delay some COVID-19 test results due to a cyberattack in mid-March 2020.

EUROPOL has confirmed that almost all of its 27 member countries have reported intensifying cyberattacks on its healthcare systems. Criminal hacker groups have demanded ransom from hospitals dealing with overload from coronavirus patients by locking their patient records, and threatening to publish these records online. This causes further unwanted strain on healthcare systems. This trend of cyberattacks done by criminal hacker groups and possibly state-sponsored actors is set to continue.

Harnessing Cyber Norms

Hospitals and healthcare providers were prime targets even before COVID-19 because cyber security was not prioritised. In light of COVID-19, cyber security

concerns may have been further deprioritised because of the lack of capacity in dealing with the pandemic. Consequently, healthcare providers are under immense pressure to pay ransoms.

There is a reason why these are termed as critical infrastructure, and states have an obligation to protect them. These obligations include honouring those previously agreed to ensure normative responsible state behaviour in cyberspace. There have been several processes like the Global Commission on Cyber Stability (GCSC) and the Paris Call that have proposed norms to protect critical infrastructure and the core of the Internet.

But none of these processes have the multilateral standing of the norms those recommended by the United Nations Group of Governmental Experts (UNGGE) in 2015, later endorsed by all the United Nations member states.

Among other things, United Nations member states agreed to protect their critical infrastructure (which in most states included healthcare); not allowing their territory to be used for internationally wrongful acts using information and communications technologies (ICTs); not supporting any ICT activity that damages the critical infrastructure of another state; for states to respond to appropriate requests for assistance by another state when it is subject to malicious ICT acts; and, for states to cooperate against cybercrime (such as ransomware attacks) and terrorism.

All For One, One For All

These obligations therefore call upon states to cooperate among themselves to prevent these cyberattacks from taking place from within their territory and share information with other states on impending cyberattacks.

These norms are particularly relevant now against the COVID-19 scourge that affects all states. States should be clear-minded that the COVID-19 pandemic does not respect state boundaries or geopolitics, seniority or youth. Healthcare systems around the world should be afforded the protection to prevent the further spread of the COVID-19.

As seen with many states badly affected by COVID-19, death rates in an overwhelmed healthcare system are exponentially higher than those that have spare capacity, and every ounce in capacity is needed to deal with the pandemic.

COVID-19 arguably represents the best opportunity for UN member states to cooperate in line with the agreed cyber norms, to build confidence and capacity among states, and strengthen adherence to these obligations to combat a common foe.

What Can Governments Do?

Confidence and capacity building measures to ensure stability in cyberspace can be undertaken domestically and internationally. Domestically, governments can take basic steps by increasing resources to mitigate cyberattacks. Some states have in the past allowed cybercriminals to operate discreetly in their territory, with hope that their expertise may be utilised in other strategic operations.

But this practice should now be stopped in light of COVID-19. Cyber criminals in any given territory that target the healthcare sector in any other state should not be sheltered or tolerated and should face harsh penalties because there are lives at stake.

International actions are more complex and require political will to execute. The 2015 norms are silent on how cooperation among member states should look like. The decision to implement cooperation is left largely to the states. But in the face of a global pandemic, the urgency of the circumstance should lend itself to a deeper and more meaningful cooperation.

In short, UN member states should hold each other accountable to these cyber norms of behaviour. They should increase resource allocation to cybersecurity protection and share best practices and timely information (like the Czechs), so that critical infrastructure like healthcare can function unhindered.

Any state that carries out or enables others to carry out cyber operations on other states' healthcare systems during this crisis must be aware of the potential for huge loss of life, which may amount to an act of war. States should therefore be called upon as responsible state actors to cooperate in investigating, locating, arresting, and prosecuting cybercriminals who use the lack of international agreements to evade capture.

Post-COVID-19: Improving State Behaviour in Cyberspace

The COVID-19 pandemic shows the importance of governments to be able to protect their critical infrastructure from malicious actors. Governments can do much more, especially after the pandemic, in order to ensure cyberspace remains safe and secure.

States need to work harder towards cooperation. The two processes – the Open-ended Working Group (OEWG) and the latest round of the UNGGE – on international security with regard to cyberspace at the United Nations are prime avenues for such cooperation to take place. When these meetings resume after the COVID-19 crisis subsides, states should strongly consider strengthening the application of norms around critical infrastructure protection.

This includes taking swift and firm action against malicious threat actors (cybercriminals or state-sponsored actors) in cooperation with each other; collectively protecting critical infrastructure around the world; and voicing out acts of irresponsible behaviour by states. Capacity and confidence building measures in cyberspace to ensure that critical infrastructure around the world would also be welcome to better equip all states with the means to tackle future crises.

To ensure that no crisis is ever wasted, UN member states can use the COVID-19 crisis to rally around these issues on the universal applicability of norms. They should also build capacity and confidence among themselves to strengthen critical infrastructure protection to better guide the behaviour of states in cyberspace.

This momentum may lead us to a safer and more stable cyberspace. Failing to do so fails the entire population that rely on critical infrastructure for survival.

Eugene EG Tan is Associate 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 (NTU), Singapore. This commentary by the CENS/FIT (Future Issues & Technology) research cluster is part of an RSIS Series.

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