Article
DIGITAL RISK : THE RISE OF CYBERATTACKS AND ITS IMPLICATIONS FOR MALAYSIA

By Umar Zainol Rahim

Since the infamous Stuxnet[1] attack on Iran's nuclear power plant in 2010, cyberattacks are fast becoming a cause for concern in national security. Its discovery was a turning point in modern warfare, especially in showcasing the extent of damage cyberattacks could potentially have on a nation's infrastructure. In the case of Stuxnet, the inherent nature of its virus was to specifically target Programmable Logic Controllers (PLCs) within the nuclear facility, which led to the disruption and eventual destruction of centrifuges tasked to separate nuclear material.

While Stuxnet was directly focused on the demolition of Iran's nuclear facility, other forms of cyberattacks are subtler in causing damage particularly with regards to a nation's credibility. In response to the release of "The Dictator" (a 2014 American satirical film centred on a scathing depiction of North Korea's Kim Jong-Un), North Korea was widely believed to have launched a cyber-attack on Sony Pictures where a large amount of confidential data was leaked. During the 2016 United States presidential election, Russia was accused of leaking incriminating communications within the Democratic National Party, which led to a number of high-profile resignations including its chairperson Deborah Wasserman-Schultz. Arguably, this leak was instrumental in securing the nomination of Donald Trump.

The scope of damage may vary in each case, but the crucial aspect here is how these attacks differ from conventional espionage operations. Firstly, cyberattacks may not require a single conventional soldier to administer. Secondly, cyber-

[1] In 2010, a highly sophisticated computer virus was discovered in Belarus. This virus, widely known as Stuxnet, was revealed to be responsible for the destruction of alleged nuclear power plants in Iran in the same year. In the process, it affected other computer systems worldwide. A comprehensive look at the Stuxnet virus can be found on: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

attacks take full advantage of the anonymity of the Internet, thus rendering it nearly impossible to trace its source. Even to this day, details of the Stuxnet attack are highly classified and there are only speculations on who or what nation-state was responsible for it. Thirdly, cyberattacks sponsored by nation states introduce new levels of technological sophistication that poses new challenges to cyber defence agencies.

It is these three elements, coupled with the potential damages of viruses that should alarm governments. For starters, questions on the efficacy of national cyber defence arise: Are countries equipped to face this emerging threat, and what are the relevant agencies/ministries tasked to oversee cybersecurity?

In the case of the United States, Barack Obama[2] showed his commitment to cyber defence, where he stressed the need for "*companies running [US] critical infrastructure [to] meet basic, common sense cybersecurity standards, just as they already meet other security requirements*". This later manifested itself in the Cybersecurity Act 2012 which appointed the US Department of Homeland Security to assess and mitigate cybersecurity risks. Furthermore, the US has also established the US Cyber Command to work alongside with the National Security Agency to provide relevant policies related to cyberspace security.

For Malaysia, the responsibility of national cybersecurity falls under Cyber Security Malaysia, an agency formed under the Ministry of Science, Technology and Innovation (MoSTI). In 2016, Defense Minister Hishammuddin Hussein lauded Malaysia's advancements in cybersecurity by proclaiming it as "among the top countries in [the ASEAN] region which is up to speed in terms of cyber defense"[3]. However, the minister added that the cyber defense system is only 90 percent complete after three years of work. With the unlimited potential state-developed worms and viruses pose, a 10 percent gap should be closed immediately as it still leaves a risk too big for national security to consider.

The second issue that arises is the response to cyberattacks, particularly those coming from outside the country. Even if the attacker had been determined without a

[2] Obama, Barack. "Taking the Cyberattack Threat Seriously." *The Wall Street Journal*. Dow Jones & Company, 19 July 2012. Web. 24 Feb. 2017. <https://www.wsj.com/articles/SB10000872396390444330904577535492693044650>.

[3] Parameswaran, Prashanth. "Malaysia's Cyber Defense: One of ASEAN's Best?" The Diplomat. The Diplomat, 26 Oct. 2016. Web. 24 Feb. 2017. <http://thediplomat.com/2016/10/malaysias-cyber-defense-one-of-aseans-best/>.

doubt, what then? What is the appropriate reaction by governments should it be found that a foreign country was responsible for a data breach? Even worse, does a cyberattack aimed at dismantling our national institutions and/or infrastructure constitute as an act of war?

The answer to these questions is a short and humbling one: nobody really knows for sure. The US government to this day has yet to define policies surrounding cyberwarfare despite years of discussions and being at the receiving end of multiple cyberattacks. During its 2016 Summit, NATO agreed to recognise cyberspace as a 'Domain of Warfare'. The implication is an important one; a cyberattack aimed at NATO countries could trigger an Article 5 response, though its details remain shrouded (Article 5 declares that an attack against one NATO member is considered an attack against all NATO members)[4]. For Ukraine, these questions must be answered immediately. In December 2015, Ukraine was the first nation to be hit with a power outage caused by a cyberattack, and again in December 2016 which amounted to a loss of about one-fifth of Kiev's power consumption at that time of night. In response, President Petro Poroshenko issued a statement accusing Russia, stating "*The investigation of a number of incidents indicated the complicity directly or indirectly of Russian security services*"[5]. However, Russia's denial of these claims complicates any stern diplomatic response.

The digital world is slowly revealing its double-edged nature. Indeed, as technology becomes more ubiquitous, thus lending itself to an increase in connectivity, innovation, and development for many nations, it also opens up vulnerabilities for hacking and sabotage. It is imperative for Malaysia to follow the emerging global developments in cybersecurity as its dependency in technology increases. Leaders must identify key competencies required in its respective organisations to address this issue. In this case, a more digitally-savvy culture could help mitigate the threats posed by new forms of cyberattacks. Additionally, appropriate ministries and agencies should improve collaboration with the intent of knowledge sharing. While the roles of Cybersecurity Malaysia and MoSTI are relevant in this situation, enforcement remains under the Royal Malaysia Police or even the National

[4] Bunkall, Alistair. "NATO 'not Agile Enough' to Stop Russian Hacking." Sky News. Sky News, 17 Feb. 2017. Web. 24 Feb. 2017. <http://news.sky.com/story/fallon-nato-failing-to-stop-russian-cyber-attacks-10771630>

[5] "Ukraine Power Cut 'was Cyber-attack'." BBC News. BBC, 11 Jan. 2017. Web. 24 Feb. 2017. <http://www.bbc.com/news/technology-38573074>.

Security Council. These partnerships may open new avenues to explore under the government's National Blue Ocean Strategy initiative. Finally, policymakers must develop appropriate responses, especially in the Ministry of Defence and the Ministry of Foreign Affairs, to highlight Malaysia's stance on cyberattacks on the international stage. Given Malaysia's advancements in cyber defence, it could very well be a pioneer in devising new policies for other nations to follow.

Article

THE ART AND SCIENCE OF NUDGING

By Khairiah Mokhtaruddin

"Wink, wink, nudge, nudge" was popularised in the 1970s through the British sketch, *Monty Python*. In the sketch, the comedian winks before elbowing the sides of another person in conversation – essentially 'nudging' as the words "nudge, nudge" are uttered. These verbal and physical expressions take place when one wants to share something sly or emphasise a comment in jest. Approximately 40 years later the term 'nudge' takes another dimension altogether, even to the extent of the establishment of a unit within the British Cabinet that has the task of influencing public behaviour.

The goal of public policy is to shape and regulate behaviour, done through legislation, regulation, incentives, and information dissemination. Intervention in policymaking requires making assumptions about human behaviour, specifically what encourages or deters certain behaviour. This is often derived from the traditional decision-making approach that correlates with behavioural economics, where individuals weigh their choices based on information that is readily available. New findings are now fast shifting the assumption that decisions are thoroughly made through individual rationality and timely deliberation based on available information.

Psychologists have long speculated that there are two distinct systems operating in the brain – the reflective and the

automatic[1]. Recent findings are further authenticating these predictions. The reflective and the automatic systems have their own capabilities and purposes. It is important to note that while these two systems are separate, in practice, both processes integrate seamlessly to govern human behaviour.

The reflective mind offers systematic and deeper analysis but has limited capacity to process when time is a constraint. The automatic mind, on the other hand, processes many things simultaneously, often separately and done subconsciously. Due to this, the automatic system habitually takes shortcuts and utilises biases based on social and cultural exposures. Therefore, social cognition and cultural perspectives are important influencers in decision-making. This may be the answer as to why humans, believed to be rational and having common sense, can sometimes make irrational decisions, and choose seemingly impractical options[2].

How then can we apply nudging to policy intervention? Nudge theory draws from human nature and psychology, but questions judgements and decisions made under the assumption of rationality (reflective system). Instead, it believes that some decisions are made automatically and subconsciously – utilising the automatic system[3]. Proponents of this theory in policy application believes that problems can be addressed by improving how choices are presented, essentially persuading the automatic and subconscious system to select the desired option.

In an example, when a hotel displayed a sign in the guest room that asked people to reuse their bath towels to save the environment, 35.1% did so[4]. However, when the sign used social norms by saying that most guests at the hotel recycled their towels at least once during their stay, the percentage grew to 44.1%. The percentage increased to almost 50% when the sign said that most previous occupants of the room in which the guest was staying had reused towels at some point during their stay. Framing the message and highlighting social norms resulted in significant change in behaviour. It confirms that people tend to do what those around them are already doing.

[1] Kahneman, Daniel (2011) *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux

[2] Ariely, Dan (2008) *Predictably Irrational: The Hidden Forces that Shape our Decisions.* London: Harper Collins

[3] Thaler, Richard and Suntein, Cass (2008) *Nudge: Improving decisions about health, wealth and happiness.* Yale University Press

[4] Cialdini, R. (2003) Crafting normative messages to protect the environment. *Current Directions in Psychological Science* 12: 105-109

In United Kingdom (UK), nudging has progressed to the extent of having what is officially known as the Behavioural Insights Team, but unofficially referred to as 'The Nudge Unit'. Initially set up as a unit within the UK Cabinet Office in 2010, it is now a limited company – owned by the UK government and Nesta (a registered leading innovation charity in the UK). Its very foundation still anchors heavily on applying behavioural sciences, ensuring that choices presented by policymakers must acknowledge the human cognition and aspects of psychology. Policymakers and multilateral organisations who have been involved in policy interventions and providing recommendations are now acknowledging this further. For instance, the World Banks' World Development Report 2015: Mind, Society, and Behaviour[5], highlights three principles of human decision-making that affects behaviour; – *thinking automatically*; *thinking socially;* and *thinking with mental models*.

The World Bank report concurred previous findings that people often receive more information than they can process, and managing information can pose some challenge in decision-making. In response, mental shortcuts are utilised much of the time. Therefore, adjusting what information is provided and how it is presented can help people make better decisions, essentially aiding the process of thinking automatically.

The second principle is based on the idea that human beings are influenced by preference, networks, identities, and norms that are inherently social in nature. Therefore, social networks and social norms that shape behaviours can serve as means of innovative interventions. Thirdly, mental models are derived from social interactions and social beliefs and practices. These mental models heavily influence individual perceptions and interpretations. Therefore, policies that provide opportunities for an alternative understanding of the world – a change in basic assumptions can expand the existing mental models, thus allowing opportunities to weigh unconventional choices.

What relevance is this insight to the Malaysian context? Plenty. Issues such as crime and antisocial behaviour; environmental sustainability; and healthcare pose serious problems for the government, problems that are further compounded in this period of shrinking resources and fiscal constraints. Therefore,

[5] World Development Report (2015) *Mind, Society, and Behaviour*. World Bank Group

efforts to encourage or deter certain behaviour must be innovative, resource-effective. It is important for policymakers to understand how different systems are utilised by people, incorporating the social and cultural contexts, and how these affect their actions. An enlightened outlook on human decision-making processes can steer policy actions into manageable and economical yet successful outcomes.

As with any approach in policymaking, there are bound to be points of contention. Of the more obvious and controversial aspect of this approach is the ethical one, where it can be argued that the approach has roots in paternalism – influencing individual choices through intervention and manipulation. Proponents of this approach, however, believe that the state has the responsibility of intervening when necessary to ensure that the choices made will lead to positive outcomes. For instance, placing healthy food at an eye level on store shelves to influence more people to select those healthier options that can lead to improved public health.

There is, however, the danger of designing 'one size fits all' solutions. We cannot ignore the contextual aspects of behavioural change. What worked in one area may not be successful in another. Detractors of this approach have also questioned its sustainability – whether changed behaviours will last or are they mere 'quick wins', or worse, with negative implications eventually.

The approach also requires rigorous testing and experimentation and this may incur some cost and take time. However, its proponents argue that the cost is minimal if compared to amending or recovering from a failed traditional policy intervention. Most importantly, nudging is simply an additional repertoire to the existing policy tools such as regulation and access to information. Its application could aid in changing behaviour, but sometimes this is not enough. A government may be able to encourage healthy eating practices by nudging towards eating five portions of fruit a day or using less fat, but it cannot ignore the need to address barriers such as the lack of supply of fresh, nutritious, and affordable food.

In Monty Python, the comedian's verbal and physical gestures served to subtly steer the conversation to his own thoughts. Similarly, the nudge approach is a powerful one if implemented well enough that it can influence the public to make better choices. Small but smart policy changes grounded in behavioural insights can make a difference.