RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 138 – 7 June 2016

Threats of Driverless Vehicles: Leveraging New Technologies for Solutions

By Muhammad Faizal Bin Abdul Rahman

Synopsis

New technologies, such as autonomous vehicles, will change the way Singapore work, live and play; yet they also present opportunities for terrorists to innovate their modus operandi. Security agencies need to stay ahead by leveraging new technologies to address nascent threats.

Commentary

THE UK SKY News reported on 6 January 2016 that Islamic State (IS) had tested a driverless car bomb. It showed a video that Sky News received from the Free Syrian Army (FSA) after it was seized from a captured IS militant. The video purportedly showed IS scientists testing the modified vehicle in Raqqa, Syria.

This chilling revelation, if confirmed, demonstrates IS' intent, if they have the resources, to devise innovative methods of conducting attacks abroad. It also certainly demonstrates IS' intent to deploy driverless vehicle-borne improvised explosive device (VBIED) when the technology is viable. A NATO official, Dr Jamie Shea, had stated that IS' experimentation with driverless VBIEDs is a worrying development.

Driverless VBIED – A Physical and Cyber Threat

Sceptics may dismiss the notion of driverless or autonomous VBIEDs as far-fetched, but this nascent technology has entered the realm of practical applications and policy making. New technologies such as driverless vehicles will eventually become common and potentially dual-use.

Closer to home, Singapore has embarked on a Smart Nation journey to harness info-communications technology for the benefit of its people and businesses. Among the efforts is Smart Mobility which includes harnessing autonomous vehicle (AV) technology. In line with this effort, the Ministry of Transport envisages a future transport system where driverless vehicles enhance our mobility and productivity, and overcome manpower constraints (for e.g. bus drivers and taxis).

The Land Transport Authority has begun testing the technology and working on a framework on safety standards for driverless vehicles on Singapore's public roads. At the present rate of progress, industry experts believe that highly autonomous vehicles will be viable by 2020 and fully autonomous (driverless) ones will be common by 2030. This is definitely not a distant future, and we are likely to witness this evolved transport scene especially given our rising life expectancy.

A terror attack in Singapore involving driverless VBIEDs is thus a plausible scenario and not a distant threat; given the rate of technology progress, how fast the country embraces new technologies to improve liveability and economic competitiveness in a globalised world, and prevalence of terrorism (by non-state and state actors) throughout human history.

The potential weaponisation of driverless vehicles was first brought to light by the Federal Bureau of Investigation (FBI) after Google rolled out its driverless car prototype. They assessed that the risk of cyber-criminals hacking into cars is very real. In a bulletin dated 17 March 2016, the FBI reiterated this risk and highlighted that while there have been no reported incidents, researchers were able to commandeer cars remotely by exploiting wireless communications. In the study cited by the FBI, researchers had used Wi-Fi to access a vehicle's electronics and manipulate its engine, steering and braking functions.

Indeed, the threat of driverless VBIEDs will be existential when there is a confluence of public use of driverless vehicles in the foreseeable future, terrorist intent (as seen in abovementioned IS video), and terrorist capability either through its own R&D or collusion with cybercriminals. Thus, the use of driverless vehicles for nefarious purposes should be a concern that warrants careful risk assessment by both counter-terrorism (CT) and cybersecurity agencies.

Possible Solution: Next-Gen ERP

Singapore's security agencies need to explore how other new technologies that may form part of the future transport ecosystem could be applied to counter the nascent threat of driverless VBIEDs. For example, agencies could leverage the Next-Generation Electronic Road Pricing System (ERP) as a powerful tool for intelligence and investigations. During the Committee of Supply Debate 2016, Minister for Home Affairs K Shanmugam had said that all available resources, such as the ERP system, have to be used to counter threats.

The Next-Gen ERP will be implemented from the year 2020 onwards, and will use the Global Navigation Satellite System (GNSS) in place of physical gantries. The intelligent system will allow for several functions including distance-based road

pricing and disseminating traffic information. Notably, the system could theoretically track all registered vehicles (including driverless ones) in Singapore for real time surveillance and capture vehicle movements in a database – a potential intelligence resource for security agencies.

Security agencies could spend the next five years working closely with transport agencies to study and determine how the Next-Gen ERP could be leveraged for the benefit of Singapore's security. For example, the vehicle movement data recorded in the ERP database could be analysed to detect abnormal patterns that may suggest terrorist or other suspicious activities (e.g. detection of stolen vehicles near high value targets, or vehicle with a physical description that does not match vehicle particulars in the ERP system); and facilitate post incident investigations. In principle, this would be similar to the existing licence-plate tracking programme established by the US Drug Enforcement Agency to tap a vehicle movement database for investigation purposes.

Security agencies thus need to stay ahead of the game by working closely with other government agencies to explore how these technologies (e.g. Next Gen ERP) could be leveraged to counter emergent threats and address challenges that could impede security efforts. At the policy-making level, agencies will need to pre-empt and address possible legislative issues such as admissibility of digital evidence in court, privacy concerns among Singaporeans and abuse of data by those with privileged access to the system.

Muhammad Faizal bin Abdul Rahman is a Research Fellow with the Homeland Defence Programme at the Centre of Excellence for National Security (CENS), a unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg