GlobalResearch
Center for Research on Globalization

Modern Merchants of Death: Spyware and Human Rights

By Dr. Binoy Kampmark
Global Research, May 15, 2019

Region: Middle East & North Africa
Theme: Intelligence, Police State & Civil Rights

Arms manufacturers of old, and many of the current stable, did not care much where their products went. The profit incentive often came before the patriotic one, and led to such dark suspicions as those voiced by the Nye Committee in the 1930s. Known formally as the Special Committee on Investigation of the Munitions Industry, the US Senate Committee, chaired by US Senator Gerald Nye (R-ND) supplies a distant echo on the nature of armaments and their influence.

The Nye Committee had one pressing concern: that the United States might fall for the same mistake it did in 1917 in committing to a foreign conflict while fattening the pockets of arms manufacturers. As Chairman Senator Nye promised,

> "When the Senate investigation is over, we shall see that war and preparation for war is not a matter of national honour and national defence, but a matter of profit for the few."

Despite the current sophisticated state of modern weaponry, along with modern offshoots (cybertools, spyware, the use of malware), the principle of ubiquitous spread is still present. Companies in the business of developing malware and spyware, modern merchants of disruption and harm, face charges that their products are being used for ill, a nastiness finding its way to hungry security services keen to monitor dissent and target contrarians. While the scale of their damage may be less than those alleged by Nye's Munitions Committee, the implications are there: products made are products used; the ethical code can be shelved.

The NSO Group, a tech outfit based in Herzliya, a stone's throw from Tel Aviv, specialises in producing such invasive software tools as Pegasus. The reputation of Pegasus is considerable, supposedly able to access data on targeted phones including switching on their cameras and microphones.

NSO's spyware merchandise has now attained a certain, viral notoriety. When Mexican investigative journalist Javier Valdez Cárdenas was butchered in broad daylight on a street in Culiacán, the capital of the Mexican state of Sinaloa, something reeked. The killing on May 15, 2017 had been designated a cartel hit, an initially plausible explanation given Valdez's avid interest in prying into the affairs of organised crime in Sinaloa. But the smell went further. As Mexican media outlets reported in June 2017, the government of former president Enrique Peña Nieto had purchased the good merchandise of Pegasus. Three Mexican agencies had purchased spyware to the tune of $80 million since 2011.

Since then, Canadian research group Citizen Lab, in collaboration with Mexican digital rights outfit R3D and freedom of expression group Article 19, have made the case that the widow of the slain journalist, Griselda Triana, became a target of Pegasus spyware within 10 days of her husband's death in 2017. According to the report, she was also targeted "a week after infection attempts against two of Valdez's colleagues, Andrés Villareal and Ismael Bojórquez." The group behind the infection attempts, named RECKLESS-1, is alleged to have links with the Mexican government.

Canadian-based Saudi dissident Omar Abdulaziz can also count himself amongst those targeted by Pegasus. In 2018, he claimed that his phone was tapped by NSO-made spyware, leading to a gruesome implication: that the Saudi authorities would have had access to hundreds of messages exchanged with the doomed Saudi journalist and fellow comrade-in-dissent Jamal Khashoggi.

In December, a suit was filed in Israel by Abdulaziz's representatives Alaa Mahajna and Mazen Masri, alleging that the NSO Group had hacked his phone in the service of Riyadh. In court papers, it was alleged that the dissident was harangued by the same individuals behind Khashoggi's murder, insisting that he pack his bags and return to Saudi Arabia.

Buried in the court documentation was the receipt of a text message purportedly tracking the shipment of a package; instead, it masked a link to the NSO Group. Once clicked, the link installed the spyware, turning the phone into an effective agent of surveillance. Soon after this took place, Abdulaziz's family home in Jidda was raided by Saudi security forces. Two brothers were subsequently detained.

Last January, Maariv, an Israeli daily, investigated reports about telephone spyware supposedly used to bug the phone of the murdered Khashoggi. Khashoggi's ending at the Saudi embassy in Istanbul, facilitated by a death squad, was not handiwork NSO wanted to be associated with. The group had been, according to a statement in December, "licensed for the sole use of providing governments and law enforcement agencies the ability to lawfully fight terrorism and crime". Misuse of products would lead to investigation and, depending on appropriate findings, a suspension or termination of the contract.

Shalev Hulio, the company's CEO, was clear to emphasise his humanity, before distancing himself and his company from the killing.

> "As a human being and as an Israeli, what happened to Khashoggi was a shocking murder."

Hulio was also adamant that "

> Khashoggi was not targeted by any NSO product or technology, including listening, monitoring, location tracking and intelligence collection."

Could such precise denials be inadvertent confessions?

The cooperative umbrella for Israel is broadening. It seeks allies, or at least some form of accommodation with regional powers, to counter common enemies. With Saudi Arabia and the United Arab Emirates, one common foe remains a constant: Iran. The Israeli state's

licensing of such companies as the NSO Group implicates the policy of permitting the distribution of Pegasus and such products. License their use; license their consequences. Molly Malekar, of Amnesty International's Israeli office, puts it simply:

> "By continuing to approve of NSO Group, the Ministry of Defence is practically admitting to knowingly cooperating with NSO Group as their software is used to commit human rights abuses."

Monitoring and killing dissidents and intrepid journalists tend to be nasty by-products. They, in a sense, have become the modern merchants of death, whose clients remain unsavoury regimes.

*

Note to readers: please click the share buttons below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

Featured image is from The Unz Review
